Pasi Villman

UTM-tietoturvapalvelin verkkoratkaisussa

Unified Threat Management

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Tietotekniikan koulutusohjelma
Opinnäytetyö
22.4.2012

Metropolia

Tiivistelmä

Tekijä Otsikko Sivumäärä Aika	Pasi Villman UTM-tietoturvapalvelin verkkoratkaisussa 39 sivua + 2 liitettä 22.4.2012
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaajat	Tuotepäällikkö Petri Lahti Yliopettaja Janne Salonen

Insinöörityössä luodaan kokonaisvaltainen katsaus yritysverkkojen tietoturvaratkaisun toteuttamiseen UTM-palomuurilla. Työssä perehdytään asiakasverkkojen suojaamiseen palomuurilaitteistolla, joka suojaa verkkoa usealla suojauskerroksella. Työssä käsitellään yritysten verkkojen nykyisiä uhkakuvia sekä riskien hallinnointia. Tiedon vuotaminen ulos yrityksistä ja työn tuottavuuden parantaminen nykyisten UTM:n ominaisuuksien avulla on olennainen osa yritysverkkojen rakenteellista suunnittelua, johon tässä työssä perehdytään.

Projektissa asiakasyritykselle toteutetaan UTM-palomuuriratkaisu. Projektissa esitellään nykyisten toisen sukupolven palomuurilaitteiden yleisimmät ominaisuudet ja teknologiaa niiden takana. Työssä keskitytään erityisesti FortiGaten UTM-laitteisiin. Projektissa rakennetun palomuurilaiteratkaisun käyttöönoton vaiheet ja konfiguraatio syventävät teoriaa FortiGate-laitteiden toiminnallisuudesta. Kokonaisuutena insinöörityö antaa hyvän yleiskatsauksen nykyisten UTM-laitteiden ominaisuuksista verkon ylläpitäjän työkaluna.

Toteutetun projektin vaiheet käydään läpi aina suunnittelullisesta näkökulmasta verkon ylläpitoon asti. Työssä luodaan kuva yritysverkon tietoturvan keskittämisen eduista ja verkon tietoturvan kustannustehokkaan ratkaisun käyttöönotosta.

Avainsanat	UTM, palomuuri, tietoturva, FortiGate, DLP, IPS

Metropolia

Abstract

Author Title Number of Pages Date	Pasi Villman UTM-firewall in network design 39 pages + 2 appendices 22nd April 2012
Degree	Bachelor of Engineering
Degree Programme	Information technology
Specialisation option	Data networks
Instructors	Technical Engineer Petri Lahti Principal lecturer Janne Salonen

The purpose of this final project is to give overview of network security design managed by UTM-firewall in business networks. This project aimed to implement multilayer protection provided by firewalls in a customer side network. In this final project we take a look into current threat landscape and how these threats can be managed. Controlling data leaks and increasing business productivity by using UTM-features is an important part of business network design. This project examines these features.

Project chapter introduces a customer side UTM-firewall solution. Chapter gives overview of 2nd generation firewalls and technology behind them. This bachelor thesis concentrates specially on FortiGate UTM-products. Firewall device solution installation and configuration procedures are presented and are meant to increase the knowledge about FortiGate devices and their functionality. In total this project gives overview about UTM-features as a tool for network administrator.

The project's phases are documented from planning phase to maintenance. This thesis introduces advantages and cost savings gained by centralizing network security in business networks.

Keywords	UTM, firewall, network security, FortiGate, DLP, IPS

Sisällys

Lyhenneluettelo

ActiveX	Ohjelmistokomponentti, jolla voidaan lisätä verkkosivuille interaktiivista sisältöä.
BGP	Border Gateway Protocol. Operaattoriverkkojen reititysprotokolla.
Brute force	Salaukseen kohdistuva hyökkäysmetodi, jossa salausavain pyritään murtamaan käymällä läpi järjestelmällisesti salausavaimen oletettuja vaihtoehtoja.
CIFS	Katso SMB.
CLI	Command Line Interface. Komentorivi.
CVE	Common Vulnerabilities and Exposures. Tietokanta yleisesti tunnetuista haavoittuvuuksista ohjelmistoissa.
Dictionary attack	Salausavaimeen kohdistuva hyökkäysmetodi, jossa salausavainta haetaan tunnetuista sanoista.
DLP	Data Leak/Loss Prevention. Järjestelmä datavuotojen estämiseksi ulos verkosta.
FTP	File Transfer Protocol. Tiedostojen siirtomenetelmä kahden tietokoneen välillä.
Gateway	Yhdyskäytävä, jota kautta verkkoliikenne ohjataan haluttuun loppuosoitteeseen.
HA	High Availability. Järjestelmien saatavuus palvelu katkoksista huolimatta.

Https	Hypertext Transfer Protocol Secure. Protokolla tiedon suojattuun siirtoon webissä.
Icmp	Internet Control Message Protocol. Kontrolliprotokolla, jolla lähetetään nopeasti viestejä verkkolaitteesta toiseen.
IDS	Intrusion Detection System. Tunkeutumisen havainnointijärjestelmä.
IP	Internet Protocol. Protokolla, joka huolehtii tietoliikennepakettien toimittamisesta pakettikytkentäisissä verkoissa.
IPS	Intrusion Prevention System. Tunkeutumisen esto järjestelmä.
IPSec	IP Security Architecture. Joukko protokollia web-yhteyksien suojaamiseen.
Keylogger	Haittaohjelma, joka kerää tiedon painetuista näppäimistä koneella.
LAN	Local Area Network. Sisäverkko.
Mapi	Messaging Application Programming Interface. Protokolla, jota käytetään exchange-sähköpostiohjelmissa.
Multicast	Ryhmälähetystekniikka.
QoS	Quality of Service. Verkkopalveluiden laadun takaaminen.
SMB	Server Message Block. Windows-käyttöjärjestelmien tiedostonjakoprotokolla.
Ssl	Secure Sockets Layer. Salausprotokolla tietoliikenteen salaamiseen.

Tftp	Trivial File Ttransfer Protocol. Yksinkertaistettu versio FTP:stä.
Url	Uniform Resource Locator. Merkkijono, joka osoittaa verkkosisällön sijainnin.
UTM	Unified Threat Management. Tietoturva palveluiden hallinnan yhdistäminen.
VoIP	Voice Over IP. Äänidatan siirtäminen pakettikytkentäisessä verkossa.
Vpn	Virtual Private Network. Tapa yhdistää sisäverkkoja operaattoriverkkojen yli.
Wan	Wide Area etwork. Operaattoriverkko.
Wsus	Windows Server Update Services. Windows-palvelimien rooli, joka jakaa käyttöjärjestelmäpäivitykset työasemiin.

1 Johdanto

Tietoturva on ollut jo vuosia kuuma puheenaihe IT-markkinoilla. Tietomurtojen määrä kasvaa päivittäin ja uusia uhkakuvia ilmestyy taivaalle sitä mukaa, kun nykyisiltä uhkilta pyritään suojautumaan. Ongelma ei kosketa pelkästään suuria yrityksiä, vaan tietoa varastetaan yhä useammin myös pienemmistä yrityksistä ja yksityishenkilöiltä. Useimmiten rikoksella pyritään taloudelliseen hyötyyn. Yksittäisten käyttäjien koneet eivät välttämättä ole aina teon kohteena vaan suuremman rikoksen teon välikappaleena. Verkkohyökkäyksiä varten käyttäjien koneet pyritään valjastamaan hyökkäyksen välineeksi. Suojautuminen uhkatekijöiltä vaatii aikaa ja ylläpitoa, usein näiden prosessien hallinnalle sitä ei ole, tai se on puutteellista.

Tämä insinöörityö perehtyy tietoturvan yleisimpiin riskitekijöihin sekä niiden taustoihin. Työn teoriaosuudessa käydään läpi yleisimmät tietoturvariskit yritysverkoissa sekä perehdytään yleisesti UTM-palomuuriratkaisuun yritysverkossa. Työssä esitellään lisäksi UTM-laitteiden ominaisuuksia ja niiden toimintaa. Tämän työn teorian pohjana UTM-palomuurien ominaisuuksissa on käytetty FortiGate-palomuurilaitteiden ominaisuuksia. FortiGate on UTM-laitevalmistajien parhaimmistoa ja edustaa ominaisuuksiltaan laajamittaista verkon suojausta. Työn teoriaosuudessa käsitellään yleisesti UTM-laitteiden soveltuvuutta kokonaisvaltaisena ratkaisuna yritysverkkojen suojaamiseen.

Työn projektiosuudessa esitellään ICT-House Group Oy:n asiakkaalle toteutettu UTM-palomuuriratkaisu. Projektiosuus läpikäy työn toteutuksen etenemisen aina suunnittelusta asennusten jälkeiseen ylläpitoon. Osio keskittyy voimakkaasti palomuurin konfiguraation määrittelyyn asennuksessa sekä esittelee FortiGate-laitteiden tarjoamia mahdollisuuksia verkkoratkaisuissa. Työssä käsitellään projektissa kohdatut ongelmat sekä perehdytään verkkoratkaisun edelleen kehittämiseen.

Työn taustalla on oma työnkuvani ICT-House Group Oy:ssä. ICT-House on suomalainen vuonna 2009 perustettu IT-alan yritys, joka toimittaa asiakkailleen kokonaisvaltaisen IT-infrastruktuurin. Toiminta perustuu asiakasyrityksen ydinosa-alueiden kehittämiseen ja kustannustehokkaiden ratkaisujen toteuttamiseen tietoliikennepalveluissa. ICT-

House toteuttaa laite- ja puheratkaisut, toimistosovellukset (pilvipalvelut) sekä tietoturva- ja tietoliikennepalvelut.

2 Tietoturva yritysverkossa

2.1 Yritysverkon riskitekijät

Normaalissa yrityksen päivittäistoiminnassa data liikkuu entistä enemmän ulos ja sisään yritysverkosta. Suurin osa kommunikaatiosta hoidetaan edelleen sähköpostin välityksellä, vaikka uudet menetelmät kuten esim. videoneuvottelut ja pikaviestimet ovat kasvattamassa suosiotaan. Työn ohessa moni tarvitsee Internetiä ulkoistettujen työkalujen käyttämisessä. Tällaisia työkaluja monissa yrityksissä ovat esimerkiksi verkon yli selaimella käytettävät CRM- (asiakkuuden hallinta järjestelmä) tai taloushallintasovellukset, joiden ulkoistaminen pk-yrityksissä verrattuna omalle palvelinjärjestelmille on kustannussyistä hyvinkin järkevää. Lisäksi työnteon ohessa Internetiä yrityksissä käytetään tiedonhakuun tai omaan käyttöön. Sosiaalisen median palvelut ovat nykyään suuri tietoturvariski. Suuri käyttäjämäärä näillä palveluilla on aiheuttanut rikollisen toiminnan siirtymisen hyvin voimakkaasti sosiaalisen median hyödyntämiseen. [1, s. 22–23.]

Pohdittaessa yrityksen tietoverkolle aiheutuvia riskitekijöitä, voidaan todeta suurimman osan riskeistä olevan käyttäjälähtöisiä. Verkkoon voidaan liittää sinne kuulumattomia laitteita tai verkkoon tuoda tietokoneita, jotka eivät kuulu yritykselle. Myös ulkoiset tiedonsiirtovälineet kuten esimerkiksi usb-muistitikut ovat riski, sillä näiden myötä virukset leviävät helposti yritysverkon koneisiin. Suurena ongelmana siirrettävissä medioissa ovat ns. autorun saastuneet mediat. [1, s. 16.] Markkinoilla on tarjolla sovelluksia, joilla näiden medioiden käyttö voidaan kuitenkin estää. Oman haasteensa aiheuttaa myös valvomaton sähköpostiliikenne, jolloin viruksia voidaan levittää verkkoon esim. viestien liitteinä.

Rikollista toimintaa esiintyy yhä enemmän ja ulkoisia uhkatekijöitä ei voida väheksyä. Yrityksen data, jonka rikolliset näkevät arvokkaana tai taloudellisesti hyödyttävänä, on usein tietomurtoyritysten kohteena. Toki verkon tietoturvan murtamisessa ei aina välttämättä ole kyse taloudellisista intresseistä, vaan myös tahallista vahingontekoa yrityksien verkoille tapahtuu paljon. Katkokset yrityksen tietoliikenneyhteyksissä tai palvelui-

den saatavuuksissa maksavat tänä päivänä yrityksille jopa huomattavia summia rahaa. Yrityksien haasteena on pystyä pitämään yrityksen luottamuksellinen data yrityksen sisällä. Omat haasteensa tälle asettaa työntekijöiden liikkuvuus ja datan siirtyminen laitteiden mukana yrityksen seinien ulkopuolelle.

2.2 Tietoturvariskien kehitys ja ehkäiseminen

2.2.1 Uhkien kehitys

Vuoden 2011 merkittävimpinä tietomurtoina muistetaan varmasti Sonyn Playstation Networkiin ja tietoturvayhtiö RSA:han kohdistuneet hyökkäykset. Hyökkäysten johdosta Sony joutui sulkemaan Playstation Network -palvelunsa lähes kuukaudeksi, ja n. 77 miljoona tilitietoa varastettiin palvelimilta. Sonyn on arvioitu joutuneen käyttämään vähintään 171 miljoonaa dollaria vahinkojen korjaamiseen [2, s. 5]. Myös suomalaisten tietoturva joutui vuoden 2011 lopulla voimakkaan tarkastelun alle sen jälkeen, kun CERT-FI raportoi marraskuun alussa Internetiin vuotaneesta listasta, joka sisälsi noin 16 000 suomalaisen henkilötiedot [3]. Vuosi 2011 tullaankin varmasti muistamaan tietoturvahyökkäysten vuotena.

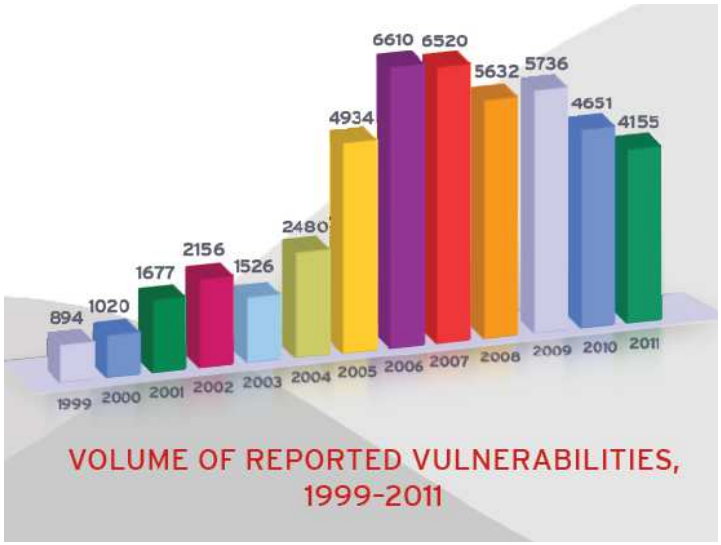
Riskien hallinta vaatii pitkäjänteistä jatkuvaa tietoturvan kehittämisprosessia. Uhkien havaitseminen etukäteen on elintärkeää yrityksen tietoturvalle. Kuitenkin useissa yrityksissä päivittäinen ylläpito ja prosessit tietoturvan tehostamiseksi ovat puutteellisia tai teholtaan riittämättömiä. Suomessa tietoturvauhkia yritykselle ei monesti haluta myöntää ja resurssien suuntaaminen ajallisesti ja rahallisesti verkon tietoturvaan nähdään tarpeettomana. Tietomurron sattuessa voi menetetyn datan arvo ja vahingon korjaaminen olla kuitenkin taloudellisesti huomattavasti kalliimpaa. Ylläpidollisesti mobiililaitteiden voimakas lisääntyminen yritysverkoissa asettaa puolestaan yritysten IT-osastoille monesti haasteen, kun laitteiden tietoturvatason valvonta on laitteiden määrän johdosta ajallisesti mahdotonta.

SophosLabsin tutkimuksen mukaan 85 % kaikista haittaohjelmista on lähtöisin verkosta. Arviolta yli 30 000 verkkosivustoa saastuu päivittäin, ja noin 80 % näistä sivustoista ovat oikeita verkkosivustoja [1, s. 10]. Ongelmana yrityksen tietoturvalle on verkon

käyttäjien huoleton asenne, kuten F-Securen tietoturva asiantuntija Erkki Mustonen asian esittää:

> Ihmiset luottavat käyttämiensä internetpalvelujen tietoturvaan eivätkä siten usko omien tietojen olevan vaarassa joutua vääriin käsiin. Salasanojen vaihtaminen koetaan myös työlääksi eikä tietovuotoja ole koettu riskitekijäksi monenlaisesta valistuksesta huolimatta. [4, s. 15.]

Tutkittaessa CVE-haavoittuvuuksien määrällistä kehitystä huomataan, että vaikka haavoittuvuuksien määrä on ollut pienessä laskussa viimeisen kahden vuoden aikana, on tiedossa olevien tietoturvahaavoittuvuuksien määrä kuvion 1 mukaisesti lähes kaksinkertainen vuoteen 2004 verrattuna.



Kuvio 1. CVE-haavoittuvuuksien kehitys 1999-2011 [2, s. 11].

Haittaohjelmilla saastuneiden koneiden määrän kasvaessa on yrityksen tietoturvan kannalta yhä olennaisempaa, että saastuneet koneet pystytään ajoissa havaitsemaan ja laitteiden liikennöinti verkossa estämään. Tietoturvayhtiö Kasperskyn tietoturvalaboratorion Internetissä julkaiseman datan mukaisesti päivittäin jopa 3,7 miljoonaa laitetta raportoi altistumisesta viruksille tai muille haittaohjelmille. Liitteessä 1 on esitetty Kasperskyn tietoturvalaboratorion statistiikka raportoiduista tietoturvaongelmista helmikuussa 2012.

2.2.2 UTM-ratkaisujen tarve

UTM-laitteiden toiminta rakentuu nykyaikaisten tilallisten (stateful) palomuurien tekniikan päälle. Laitteiden toiminnan perimmäisenä ideana on, että yritysverkkoon sallitaan liikenne vain verkkoyhteyksille, jotka on käynnistetty verkon sisältä. Oletuksena kaikki ulkoapäin sisäverkkoon suunnattu liikenne on estetty.

Tarve niin sanotuille uudensukupolven palomuurilaitteille on syntynyt, koska nykyiset haittaohjelmat muuntautuvat kiivaalla tahdilla ja uusia uhkia ilmestyy kymmeniä tuhansia päivässä. Työasemien virustorjuntaohjelmistojen on lähes mahdotonta pysyä mukana tällaisessa tahdissa. Tämän myötä yritykset ovat halunneet lisätä verkkoihinsa enemmän suojakerroksia. Nykyisin ongelmana perinteisille palomuureille on, että tietoturvauhkat ovat aivan eri tasolla verrattuna muutamia vuosia sitten vallinneeseen tilanteeseen. Tämän päivän verkkosuojauksessa ei riitä, että liikenteeltä suljetaan tiettyjä portteja tai IP-osoitteille tehdään muunnoksia, koska useimmiten käyttäjät houkutellaan suoraan rikollisten hyökkäyssivustoille. Perinteisillä palomuuriratkaisuilla ei pystytä tarjoamaan varsinaista suojaa verkolle senkään vuoksi, että nämä laitteet eivät ymmärrä liikenteen sisältöä. [5, s. 50-51.]

Nykyaikainen UTM-palomuuri on myös yrityksen verkonhallinnan kannalta helppo ratkaisu. UTM-laitteiden avulla pystytään tehokkaasti parantamaan verkon kustannustehokkuutta, kun kaikki tarvittavat verkon suorituskykyä ja turvallisuutta edistävät toiminnot voidaan keskittää verkossa yhdelle laitteelle. Esimerkiksi IDS/IPS, antivirus, AC (Application Control) ja DLP-suodattimia tai kaistanhallintaan liittyviä palveluita ei tarvitse toteuttaa erillisinä ratkaisuina omilla laitteillaan. Verkon ylläpitäjän näkökulmasta kyky suodattaa Internetin ja sovellusten generoimaa liikennettä yhden laitteen avulla on kullanarvoinen.

Tietoturvaratkaisujen kehityksen tarvetta on ohjannut viime vuosina voimakkaasti yritysten halu estää yritysverkon läpi tapahtuva työnteon kannalta epäolennainen verkon käyttö. Yhä useammin yrityksissä halutaan rajoittaa sosiaalisen median palveluiden sekä pikaviestintäohjelmien käyttöä. Nucleusresearchin tutkimuksen mukaan yrityksissä, joissa Facebookin käyttö on sallittua, on tuottavuuden lasku yhden työpäivänä ollut 1,5 % [6, s. 1]. Pahimmillaan Facebookin käyttöön tai nettipeleihin voi tuhlaantua merkittävä osa työajasta. Yritysverkolle UTM-laitteiden suodatusominaisuuksien suurin vaikutus on kuitenkin tietoturvariskien ennaltaehkäisyssä. Verkonylläpitäjä voi estää käyt-

täjiä päätymästä haitallista sisältöä sisältäville sivustoille estämällä esimerkiksi aikuisviihdesivustot, pikaviestintä- ja p2p-sovellukset (vertaisverkko) sekä suodattamisen kiertoon tarkoitetut proxy-palvelut. UTM-laitteiden virustorjuntaominaisuudet ovat yrityksien verkoille arvokas lisä, sillä usein laitteiden käyttämä antivirustietokanta on eri ohjelmistovalmistajan kuin työasemien omien turvaohjelmien. Verkon tietoturvan kannalta paraskaan UTM-laite ei poista työasemien virustorjuntaohjelmistojen tarvetta eikä ylläpitoa käyttöjärjestelmien pitämiseksi ajantasaisina.

3 FortiGate UTM -palomuuri yritysverkossa

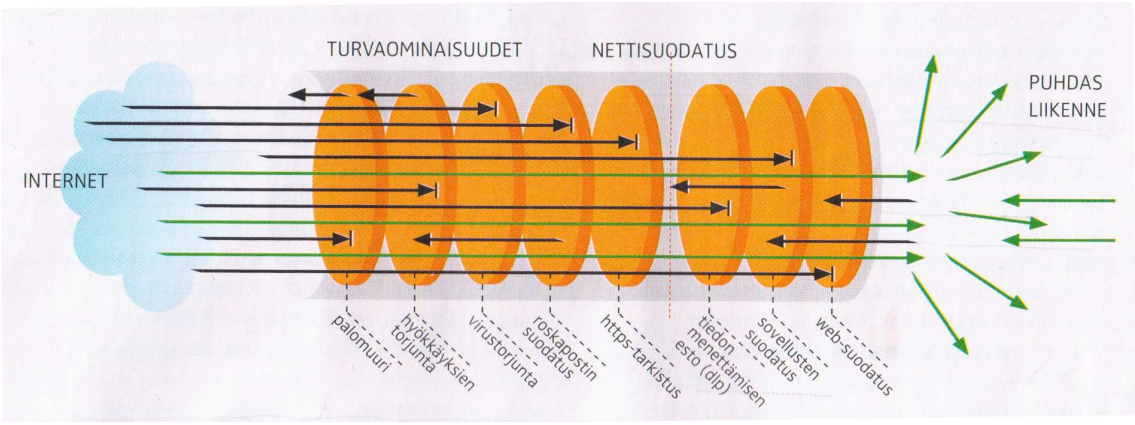
3.1 Paketin kulku palomuurissa

UTM-palomuurin avulla pyritään verkkojen kokonaisvaltaiseen suojaamiseen yhden laitteen avulla. UTM-laitteen avulla pystytään tutkimaan palomuurin läpäisevän liikenteen sisältö. Tällöin yritysverkon suojaksi pystytään rakentamaan usean sovelluskerroksen suojaus. FortiGaten UTM-palomuureissa liikenne ohjataan palomuurin läpi TCP/IP-viitemallin mukaisesti. Paketin saapuessa laitteen verkkoportille ohjataan se FortiGaten käyttöjärjestelmän (FortiOS) käsiteltäväksi ja siirrettäväksi kohti ylempiä sovelluskerroksia.

Verkkoportilta paketit ohjataan reititysmoduulille, jossa FortiOS tutkii paketin kohde-IP-osoitteen ja määrittää tarpeen prosessoida paketti. Prosessoitavat paketit ohjataan edelleen palomuurimoduulille, jossa paketin lähde- ja kohdeosoitteita verrataan palomuurisäännöstöön. Mikäli paketti on saapunut VPN-tunnelin kautta ja sen sisältö on salattu, ohjataan paketti erilliselle VPN-moduulille ennen kuin se ohjataan palomuurimoduuliin. Paketit, jotka täyttävät jonkin sallivan palomuurisäännön, ohjataan lopuksi ohjelmamoduulin tutkittavaksi. Tässä vaiheessa mukaan tulevat palomuurisääntöön liitetyt ennalta määritetyt UTM-ominaisuudet ja niiden hyödyntäminen. Palomuurisääntöjen avulla voidaan sääntökohtaisesti määrittää käytettävät UTM-ominaisuudet. Liitteessä 2 on sivuilla 1-2 esitetty prosessikaavio liikenteen reitittämisestä FortiGate-palomuurin eri moduulien välillä.

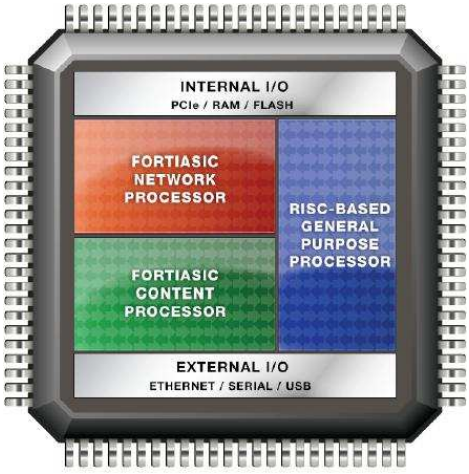
3.2 Liikenteen suodatus

Halutuimmat tietoturvaominaisuudet UTM-laitteilta ovat yleensä antivirusskannaus ja IPS-suodattimen käyttö. Monesti myös DLP, AC ja sähköpostiprotokollien suodattimet sekä kaistanhallinnan ja laadun määrittelyt (traffic shaping, QoS) ovat ominaisuuksia, joilla verkon tietoturvaa ja käytettävyyttä halutaan nostamaa. Kuviossa 2 on havainnollistettu liikenteen kulkua eri suojauskerrosten läpi UTM-palomuurissa.



Kuvio 2. UTM-palomuurin liikenteen suojauskerrokset [5, s. 52].

Monesti ajettaessa liikenne usean suojauskerroksen läpi vaaditaan laitteelta huomattavaa suorituskykyä, jotta liikenteelle aiheutuva viive jäisi mahdollisimman pieneksi. Viiveiden kasvu aiheuttaa nopeasti ongelmia esimerkiksi VoIP-puheluissa. FortiGaten UTM-laitteiden suorituskyky perustuu prosessoinnin jakamiseen eri käskykantoihin. Erillinen verkonliikenteen hallintaan liittyvä käskykanta mahdollistaa verkkoliikenteen ja VPN-yhteyksien kiihdyttämisen laitteistossa käytettävän raudan avulla. Käytetty teknologia perustuu Intelin ja AMD:n valmistamiin prosessoreihin. Tietoturvasyistä valmistajat eivät ilmoita tarkkoja kuvauksia käytetyistä teknologioista. Kuviossa 3 on esitetty FortiGate UTM -palomuurin prosessointirakenne.



Kuvio 3. FortiGate-prosessointirakenne [7, s. 8].

3.2.1 Antivirus ja web-suodatus

Antiviruksen toiminta perustuu FortiGaten UTM-muureissa Fortinetin omaan virustietokantaan. Virusskanneri etsii verkkoliikenteestä tietokannan mukaisia virustunnisteita sisältävää liikennettä. Virusskannausta voidaan tehdä FortiGaten palomuureissa joko puskuroituna tai lennosta. Puskuroidussa skannauksessa ladataan koko paketti palomuurin puskurimuistiin, jossa paketin sisältö tarkistetaan kokonaan. Lennossa tapahtuvassa skannauksessa liikenne ohjataan eteenpäin sitä mukaa, kun paketin sisältöä luetaan. Puskuroidulla virustarkastuksella pystytään havaitsemaan lennossa suoritettavaa tarkistusta enemmän viruksia, koska lennosta suoritettava tarkistus pystyy tutkimaan vain pienen osan paketin sisällöstä kerrallaan, eikä pysty purkamaan useita pakkauskerroksia. Etuna lennossa suoritettavassa tarkistuksessa verrattuna puskuroituun skannaukseen on parempi suorituskyky sekä rajoituksettomuus skannattavan tiedoston koolle. FortiGaten UTM-palomuureissa antivirus toimintoihin voidaan konfiguroida käyttöön myös grayware- ja heuristinen skannaus [8, s. 787]. Liitteessä 2 sivuilla 3-4 on esitetty prosessikaaviot FortiGaten antiviruksen puskuroidulle ja lennosta tehtäville skannauksille.

Web-suodatuksen toiminta FortiGaten UTM-palomuureissa voidaan jakaa kolmeen osaan. Nämä osat ovat sisällön suodatus, URL-suodatus sekä FortiGuardin web- suodatus. Sisällön suodatuksella suodatetaan pois www-sisältö, joka sisältää sanoja tai lauseita, jotka halutaan estää. URL-suodatuksella voidaan estää haluttuja sivustoja lisäämällä tietty sivusto tai yksittäinen verkkosivu estolistalle. FortiGuardin suodatus perus-

tuu Fortinetin tietoturvalaboratorion Internet-sivustoille annettuun luokitukseen. Suodattimella voidaan esimerkiksi estää rasististen sisällön luokituksen saaneet sivut palomuurin konfiguraatiossa.

FortiGaten UTM-laitteiden web-suodatus toimii kerrosten läpi seuraavassa järjestyksessä:

1. URL-suodatus
2. FortiGuard-sisällön suodatus
3. web-sisällön suodatus
4. web-skripti suodatus
5. virusskannaus sisällölle.

URL-suodattimen avulla pystytään estämään tai sallimaan liikenne haluttuihin sivustoihin tai IP-osoitteisiin. URL-suodattimella voidaan tarvittaessa määrittää luotetut sivustot ohittamaan (pass) suoraan muut verkkosivun sisällön suodatuksen kohdat. Web-sisällön suodattimen toiminta perustuu sisällön pisteyttämiseen ennalta määrättyjen sanojen tai lauseiden esiintymien määrän mukaisesti verkkosivulla. Mikäli konfiguroitu raja-arvo ylitetään, estää suodatin pääsyn sivustolle.

Lisäarvona FortiGaten UTM-palomuuri tarjoaa web-liikenteelle skriptipohjaisen suodatuksen. Web-suodatuksen avulla käyttäjä voidaan esimerkiksi pakottaa käyttämään yleisimmillä hakukoneilla (Google, Yahoo, Bing) SafeSearch-toimintoa. Lisäksi ActiveX-, Cookie- (eväste) ja Java-komponenttien sekä sivustojen lomakkeiden suorittaminen voidaan estää [8, s. 856–857]. FortiGaten UTM-palomuureissa voidaan määrittää jokaiselle web-suodatin profiilille CLI-komennolla käytettävä virustietokanta. FortiGuard web -suodatuksen prosessikaavio on esitetty liitteessä 2 sivulla 5.

3.2.2 IPS ja DLP

UTM-palomuurien ominaisuuksiin kuuluu lähes poikkeuksetta aina IPS, jolla voidaan suojata verkon koneita ulkopuolisilta hyökkäyksiltä. FortiGaten UTM-palomuureissa on IPS, joka käyttää joko tilastolliseen poikkeavuuteen (anomaly based) tai tunnettuun hyökkäystapaan (signature based) perustuvaa mallia suojatessaan verkkoa ulkopuolelta kohdistuvilta hyökkäyksiltä. FortiGuardin tietokanta tunnistaa yli 5100 erilaista tun-

nettua IPS signaturea [9]. FortiGaten UTM-laite voidaan konfiguroida myös IDS-laitteeksi, jolloin palomuuri toimii verkkoliikenteen pakettien monitorina eli niin sanotussa sniffer-tilassa.

Verrattuna muihin tunnettuihin UTM-laitevalmistajiin pystytään FortiGaten UTM-palomuurilla toteuttamaan DLP-ratkaisu (data loss/leak prevention). DLP on nykypäivän kuuma alue tietoturvakehityksessä [5, s. 50]. DLP:n avulla voidaan estää yrityksen tietojen vuotaminen verkon ulkopuolelle. Vastaavasti DLP:n avulla voidaan estää verkosta tietojen hakeminen yritysverkkoon. Yleisimmin DLP-suodatuksella estetään esimerkiksi sähköpostien suuret liitetiedostot sekä suorittavien tiedostotyyppien kuten .exe- tai .bat-tiedostojen lataaminen. Myös suunnittelutyöhön liittyvien CAD-dokumenttien siirto verkon ulkopuolelle halutaan usein estää. DLP-suodatus perustuu joko tiedostotyypin, tiedostonimen tai tiedoston koon skannaukseen verkkoliikenteestä. Suodatus voidaan myös konfiguroida etsimään kryptaamattomien sähköpostiviestien sisällöstä esimerkiksi Visa- tai Mastercard-korttien numerojen esiintymiä sekä sosiaaliturvatunnuksia. [8, s. 768.]

3.2.3 Roskapostisuodatus ja ohjelmien hallinta

FortiGaten UTM-palomuurilla pystytään toteuttamaan tehokkaasti roskapostisuodatus verkkoliikenteelle. Nykyaikaisella UTM-palomuurilla voidaan tutkia myös SSL-salattu sähköpostiliikenne (SMTPS, POP3S, IMAPS). FortiGate-roskapostisuodatuksen avulla on mahdollista normaalin tietokantapohjaisen roskapostisuodatuksen (antispam) lisäksi suodattaa viestejä perustuen ennalta määritettyyn listaan sanoista, joita viesteistä etsitään. Varsinainen antispam-toiminnallisuus perustuu FortiGuardin tietokantaan. Roskapostiviestien havaitsemisessa viesteistä etsitään linkkejä, jotka kuuluvat listalle tunnetuista URL-osoitteista, joiden tiedetään olevan haitallisia tai olevan tietojenkalastelu, eli phishing-sivustoja. Lisäksi antispam-suodatin lähettää viestistä tarkistussumman FortiGuardin antispam-palvelimelle, jossa summaa verrataan tunnettujen spam-viestien tarkistesummaan. Lisäksi FortiGaten palomuuri tekee DNS (domain name system) -kyselyn viestin lähettäjän domainista, jolla tarkistetaan domainin olemassaolo sekä mx-tietuiden olemassaolo kyseiselle domainille. Viestin lähettäjän IP-osoitetta verrataan myös tunnettuihin spam-lähettäjiin. FortiGate UTM-palomuuri merkitsee oletuksena spam-viestiksi todetun viestin roskapostiksi viestin otsikkotietueeseen. SMTP- ja

SMTPS-protokollien roskapostiviestit pudotetaan oletuksena automaattisesti. [8, s. 799–802.]

Yritysverkossa toimivien ohjelmien valvonta on nykyään monimutkaista, kun ohjelmat eivät välttämättä käytä kiinteitä portteja liikennöintiin. Lisäksi ohjelmaa käyttävä päätelaite ei aina ole kiinteälle IP-osoitteelle määritetty laite. Tällöin ohjelmien valvonta perinteisen palomuurin ominaisuuksin on mahdotonta. Uuden sukupolven palomuurien avulla hallinta on kuitenkin saatu mahdolliseksi. FortiGaten UTM-palomuureisssa pystytään konfiguroimaan palomuurisääntöihin käytettäväksi ohjelmien hallinta (application sensor). UTM-palomuuri hyödyntää IPS:n protokolla dekooderia, jonka avulla se pystyy tunnistamaan verkkoliikenteen generoivan ohjelman. Palomuurilla on tällöin mahdollista estää tai lokittaa näiden ohjelmien generoima liikenne. Tietoturvan ja tuottavuuden kannalta on hyödyllistä pystyä estämään erimerkiksi Facebook, Youtube ja tiedostonjakosovellukset, sekä pikaviestiohjelmat ja muut liittymän kaistaa kuormittavat ohjelmat. FortiGate UTM -palomuurissa voidaan konfiguroida ohjelmien hallintasensoreihin kaistanhallinnallisia rajoitteita. Tällöin voidaan hallita, paljonko esimerkiksi interaktiiviset sovellukset voivat maksimissaan käyttää Internet-yhteyden kaistasta.

3.3 Reititysominaisuudet

FortiGaten UTM-palomuurit voidaan konfiguroida verkkoratkaisussa reitittimeksi. Kaikissa FortiGaten malleissa on tuki IPv6:lle ja multicastingille. Reititysprotokollina on sisäverkolle OSPF, RIPv1 ja RIPv2. Operaattoriverkkoja varten reititysprotokollista ainoana vaihtoehtona on graafisen käyttöliittymän kautta konfiguroida käyttöön BGP. Staattinen reititys voidaan toteuttaa IP-osoitteilla tai sääntöpohjaisesti protokollaperusteisesti. IS-IS-reititysprotokolla on mahdollista konfiguroida CLI:n kautta. FortiGaten UTM-palomuuri voidaan määritellä kuorman jakoa (load balancing) varten. Kuormanjako voidaan toteuttaa painotettuna (weighted) tai lähde-IP-osoitteen mukaan. FortiGaten laitteisiin voidaan kuormanjaon konfiguraatioon määrittää gatewayn tilan seuranta (Dead gateway detection).

3.4 Korkea käytettävyys ja virtuaalidomainit

Verkkojen korkea käytettävyys ja palveluiden saatavuus ovat tärkeä osa tuottavuutta. Katkokset verkkoyhteyksissä haittaavat yritysten liiketoimintaa. Verkkolaitteiden ja yhteyksien kahdentaminen on etenkin kriittisissä verkkopalveluissa kuten operaattoritoiminnassa välttämätöntä. FortiGaten UTM-palomuurit tukevat klusterointi mahdollisuutta ja laitteiden kahdentamista. Palomuurit voidaan määrittä HA (high availability, korkean käytettävyyden) -klusteriin ja määrittää toimimaan tällöin joko aktiivi-aktiivi- tai aktiivi-passiivi -tilassa. Aktiiviset klusterit voidaan rakentaa myös useammalle kuin pelkästään kahdelle UTM-palomuurille. FortiGaten UTM-palomuurit käyttävät HA-tilan seurantaan FortiGate Clustering Protokollaa (FGCP). Korkean käytettävyyden ominaisuuksien laajentaminen esimerkiksi Ciscon verkkolaitteisiin on tuettu VRRP:n (Virtual router redundancy protocol) avulla, jolloin esimerkiksi reititys voidaan siirtää vikatilanteissa laitteelta toiselle.

Nykyaikaisella UTM-palomuurilla voidaan rakentaa erillinen palomuuriratkaisu useammalle erillisille verkoille. FortiGaten UTM-laitteissa voidaan ottaa käyttöön virtuaalidomain (VDOM) -ominaisuus, jolloin yhden palomuurin rauta voidaan jakaa virtuaalisiin instansseihin. Tällöin verkon eri osille voidaan määrittää kullekin oma palomuurinsa. Ratkaisu lisää huomattavasti verkkojen kustannustehokkuutta sekä joustavuutta. Erityisesti ratkaisulla voidaan saavuttaa suuri hyöty silloin, kun esimerkiksi useamman samassa tilassa toimivan yrityksen verkot halutaan yhtenäisen tietoturvaratkaisun taakse tai laitteella halutaan toteuttaa esimerkiksi operaattoriverkossa tietoturvapalveluita loppuasiakkaille yhdellä rautatason laitteella.

3.5 Wan-optimointi ja Wlan-kontrolleri

FortiGaten UTM-palomuurilaitteilla on mahdollista optimoida kahden FortiGate-palomuurin välistä Wan-linkin yli kulkevaa liikennettä. Liikennettä voidaan optimoida protokollan perusteella tai puskuroimalla haettava data tai sivusto FortiGate-laitteeseen. Tärkeimpänä ominaisuutena on mahdollisuus optimoida CIFS-, FTP- ja MAPI-protokollien liikenne. Usein eri toimipaikkojen välillä on tarve noutaa tiedostoja esimerkiksi pääkonttorin palvelimelta sivukonttorin asiakaskoneelle. LAN-verkoissa CIFS/FTP:n käyttö harvoin aiheuttaa ongelmia, mutta siirrettäessä dataa Wan-verkkojen yli kasvavat usein latenssit ja viiveet liikenteelle pitkiksi. Tällöin voidaan työn

tuottavuutta ja verkon suorituskykyä parantaa optimoimalla esimerkiksi CIFS- tai FTP-protokollien liikennettä.

Langattomat verkot yleistyvät kovaa vauhtia ja ovat syrjäyttämässä perinteisen työasemakaapeloinnin. Yhä useammasta työasemasta puuttuu nykyisin kaapelointi liitäntä. Useat toimistot haluavat tarjota työntekijöilleen liikkuvuutta toimiston sisällä, sillä työtä ei tehdä välttämättä enää perinteisesti oman työpöydän ääressä. Langattomien verkkotekniikoiden nopea kehitys on nostanut verkon nopeudet riittävälle tasolle verrattuna kaapeloituihin yhteyksiin. Tuleva 802.11ac-standardi tulee nostamaan langattomien verkkojen siirtonopeuden 1 gigabitin tasolle. Langattomien verkkojen hallinta toimistorakennuksissa keskitetysti on houkutteleva vaihtoehto silloin kun tukiasemia joudutaan sijoittamaan useampia yrityksen tiloihin, jotta verkolla on riittävä peitto ja toimintavarmuus. Kontrolloituja ratkaisuja on monilla eri valmistajilla, mutta monesti kustannukset nousevat korkeiksi. FortiGaten UTM-laitteilla pystytään toteuttamaan langaton yritysverkko kontrolloidusti sekä tarjoamaan UTM-tason tietoturva langattoman verkon liityntäpisteille. Verkon kontrollointi tapahtuu keskitetysti palomuurista. FortiGaten palomuurit pystyvät hallitsemaan mallista riippuen 2-512 tukiaseman verkkoa kontrolloidusti. Jokaiselle tukiasemalle on mahdollista määrittää 8 SSID:tä (langattoman verkon nimi) jokaista käytettävissä olevaa radiota kohden. Wlan-kontrollerin ominaisuus, jolla voidaan havaita verkkoon kuulumattomat tukiasemat ja estää näiden liikenne on edellytys langattomien verkkojen tietoturvalle ja verkkorakenteen hallitsemiselle. Verkon liikenteen hallinnointi niin langallisissa kuin langattomissa yhteyksissä on ehdoton edellytys nykyisille tietoverkoille. Verkon rakenteen hallinta ja ylläpidon keskittäminen luovat edellytyksen palveluiden tarjoamiseen tehokkaasti ja turvallisesti yritysverkon loppukäyttäjille. Lisäksi FortiGatelta löytyy lisäohjelma langattomien verkkojen suunnitteluun ja tukiasemien sijoitteluun.

4 Projektin esittely ja toteutus

4.1 Esittely

Tämä projekti toteutettiin ICT-House Group Oy:n asiakkaalle vuoden 2011 kesän ja alkusyksyn aikana. Työssä asiakkaalle räätälöitiin tietoturvaratkaisu, jota voidaan tarvittaessa hallita itse ulkoisesta operaattorista riippumattomana palveluna omassa yritys-

verkossa. Työ toteutettiin Helsingissä sijaitsevaan organisaatioon, joka tarjoaa opetus- ja sivistyspalveluita.

Tarve ratkaisulle syntyi alun perin, kun ulkopuolisen Internet-palveluita tarjoavan operaattorin aiemmin toimittamasta yritysverkon palomuuriratkaisusta haluttiin luopua. Syynä rakennemuutokseen oli pääosin operaattorien hitaus ja kankea toiminta, kun verkon reunalla tapahtuvaan liikenteen ohjaukseen haluttiin tehdä muutoksia. Toimitetulla ratkaisulla haluttiin tuoda verkon hallinta lähemmäs asiakasta.

Muutoksen myötä myös organisaation verkon aktiivilaitteet vaihdettiin yhden gigabitin porttinopeudella toimiviin laitteisiin. Sisäverkon rakenne toteutettiin uudestaan, ja ulkoiset operaattoriyhteydet kahdennettiin tuomalla kiinteistöön toinen kuituliittymä.

4.2 Suunnittelu

Projektin suunnittelu alkoi asiakkaan nykyisen verkkoratkaisun toiminnallisuuden puutteiden kartoittamisella. Asiakkaan alkuperäiseen verkkoratkaisuun verrattuna pyrittiin suunnitelman mukaisesti irtaantumaan Internet-operaattoreiden palomuuripalveluista. Tarkoitus oli siirtyä verkonhallinnassa tilaan, jossa ainoastaan Internet-yhteyden hallinta jää operaattorille. Suunnittelun lähtökohtana oli tieto Internet-yhteyksien kahdentamisesta. Kiinteistöön tultaisiin asentamaan asiakkaalle jo olemassa olevan liittymän lisäksi toinen kuituliittymä, ja molempien liittymien nopeus tultaisiin nostamaan 500 megabitin nopeuteen. Näihin liittymiin haluttiin luotettava palomuurilaitteisto, jonka suorituskyky mahdollistaisi verkkoliikenteen suodatuksen kolmesta eri tyypin verkkorakenteesta sekä myöhemmässä vaiheessa myös VoIP-liikenteestä.

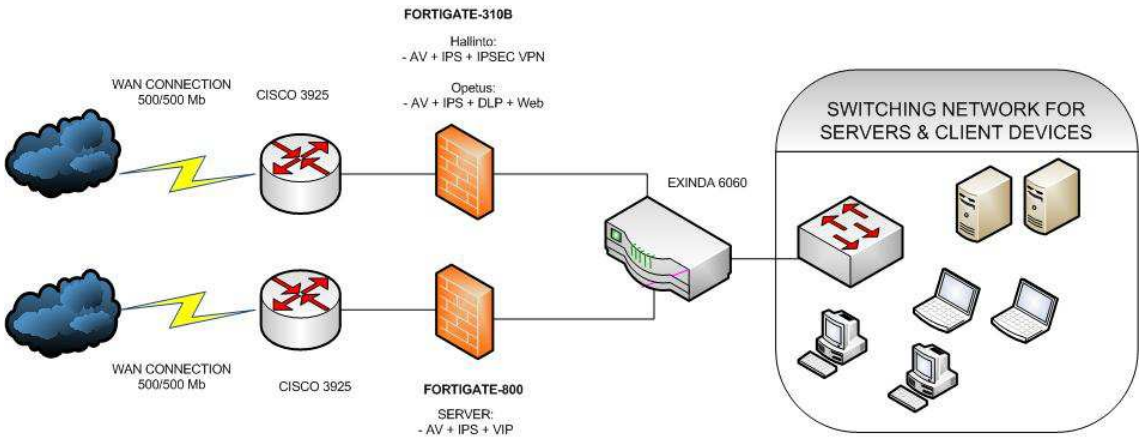
Projektin suunnittelun edetessä päädyttiin ratkaisuun, jossa hallinnollinen ja opetustoimen verkko rakennettiin alkuperäiseen jo olemassa olevaan Internet-liittymään. Suunnitellussa ratkaisussa tultaisiin myöhemmässä vaiheessa suorittamaan VoIP-integraatio verkkoon, joten tämän huomioiminen UTM-laitteiden valinnassa asetti vaatimuksia suorituskyvylle. Suunnittelun myötä verkon tulisi pystyä palvelemaan toimivasti 390 työaseman ja 18 palvelimen verkkoympäristöä. Laitteiden määrän kasvuun varauduttiin ja järjestelmä ylimitoitettiin huomioiden myös mobiililaitteet. Lisäksi suunnitteluvaiheessa haluttiin varautua verkon suorituskyvyn riittävyyteen, mikäli verkossa tultaisiin salli-

maan myös käyttäjien omat kannettavat tietokoneet, tabletit ja muut ulkoiset verkkolaitteet. Tarvittaessa verkon tulisi pystyä myös laajamittaiseen ulkoistettujen sähköisten palveluiden käyttöön.

Asiakkaan ympäristön 18 palvelinta päätettiin verkkorakenteen uudistusprojektin myötä siirtää omaksi sisäverkon segmentikseen tulevan kuituliittymän UTM-palomuurin taakse. Ratkaisulla saavutettiin verkon tälle osalle riittävä suorituskyky sekä tietoturvaltaan toimiva ratkaisu.

Verkon segmentoinnin ja topologian selkiintyessä suunnittelussa edettiin pohtimaan laitteiden suorituskyvyllistä näkökulmaa. UTM-laitteen asentamisessa verkkoliikenteen suojaksi tulee huomioida laitteen ominaisuudet. Esimerkiksi laitteen läpäisykyvystä on huomioitava suorituskyky tehtäessä liikenteelle virustarkistusta/hyökkäyksenestoa tai että riittävä määrä istuntoja pystytään avaamaan palomuurin läpi. Tiedossa oleva VoIP ratkaisu myös asetti suunniteluun oman vaikutteensa, joka johti suurelta osin siihen, että ratkaisussa päädyttiin valintaan, jossa palomuurilaitteistossa on kaistan kiihdytysominaisuudet. Varsinaista verkon liikennemäärää myös pohdittiin osana ratkaisua ja olennaisena näkökulmana pidettiin opetustoimen verkkoa, jossa tultaisiin hyödyntämään UTM-laitteen ominaisuuksia ja skannaamaan verkkoliikennettä huomattavasti muita verkkosegmenttejä enemmän. Verkon toiminnassa tämä ei saanut näkyä, joten tietoturvapalvelimen suoritusarvoja jouduttiin korostamaan entisestään, jotta toiminnallisuus suorituskyvyssä pystyttiin takaamaan. Tietoturvapalvelimille saapuva liikenne tultaisiin kiihdyttämään Exinda-kaistankiihdytinjärjestelmän läpi, joten pullonkaulaa ei tulisi muodostua verkon reunalle.

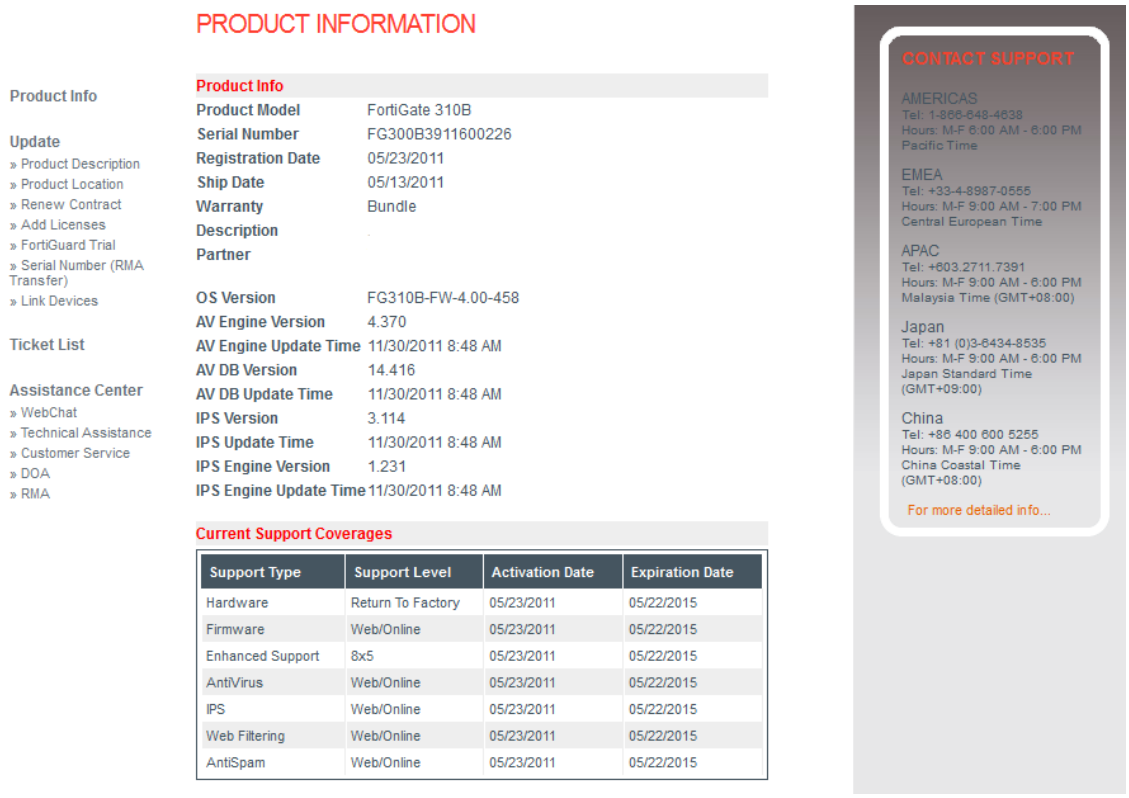
Palvelinverkolle asennettavan tietoturvapalvelimen valintaan vaikutti myös suorituskyky-kriteerit. Palvelinverkossa toimii organisaatiossa mm. opetusjärjestelmiä, keskitetty virustorjunnan hallinta, sähköposti- ja domainhallintaan liittyvät palvelut. Ratkaisussa päädyttiin lopulta asentamaan palvelinverkolle FortiGate-800 UTM -palomuuri ja hallinnon- ja opetustoimenverkolle FortiGate-310B UTM-tietoturvapalvelin. Kumpaankin tietoturvapalvelimeen liitettiin myös neljän vuoden palvelulisenssit. Kuviossa 4 on havainnoitu suunnitelma verkon topologiasta ja määritettävistä UTM-ominaisuuksista asennuksessa.



Kuvio 4. Projektin suunniteltu verkkotopologia.

4.3 Asennuksien valmistelu

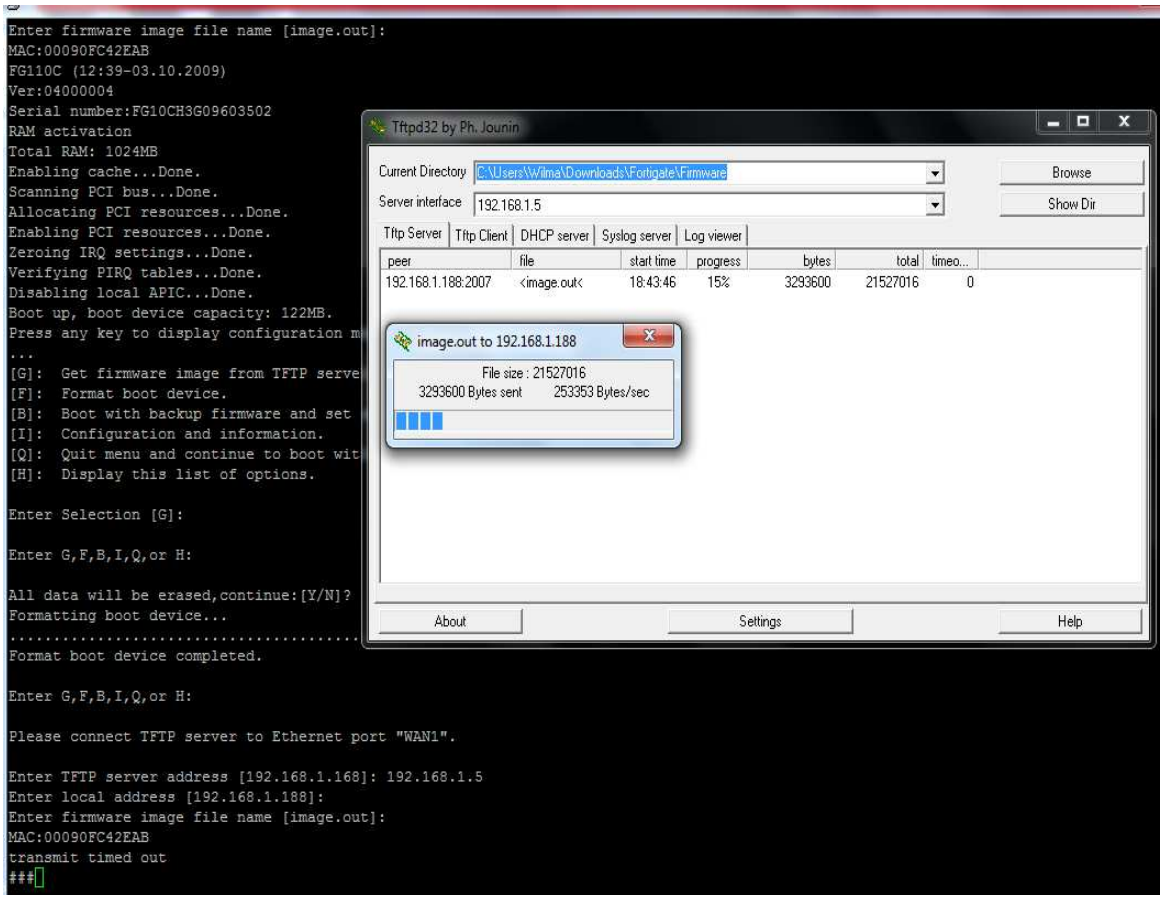
UTM-tietoturvapalvelimien esiasennus asiakkaalle aloitettiin rekisteröimällä laitteet sarjanumeron perusteella Fortinet:n palvelimille. Rekisteröinnin avulla aktivoidaan laitteisiin rautaan ja ohjelmistoihin liittyvät lisenssit sekä tuotetuki näille. Lisäksi myös tilatut UTM-palvelulisenssit aktivoidaan samalla rekisteröinnillä. FortiGaten palomuureihin liitettävät UTM-palvelulisenssit ovat aina lisenssi-bundleja eli kokonaisuuksia, jotka sisältävät antiviruksen, IPS:n, webin ja sähköpostipalveluiden sisällön suodatuksen. Palveluiden rekisteröinti tehtiin Fortinetin Customer Service&Support -portaalin kautta. Kuviossa 5 on esimerkki portaaliin rekisteröidyn laitteen yhteenvedosta.



Kuvio 5. FortiGate Customer Service&Support -portaalin rekisteröidyn laitteen tiedot

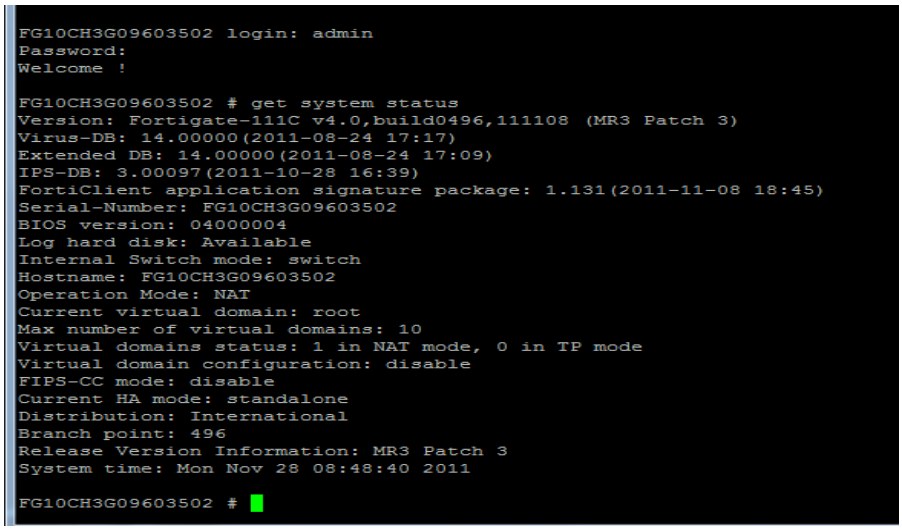
Rekisteröinnin jälkeen palomuurilaitteita varten noudettiin Fortinetin tukiportaalista palomuurien viimeisimmät ohjelmistoversiot sekä virus- ja IPS-tietokannat. Tietokantojen asennus verkkoon liittämättömiin palomuureihin tehtiin konsoliyhteyden yli käyttämällä kannettavaan tietokoneeseen asennettua tftp-palvelinohjelmistoa.

Ohjelmiston lataamista varten palomuuriin määriteltiin työasemalle kiinteä IP-osoite 192.168.1.0/24-verkosta. Lisäksi ladattavalle firmware-tiedostolle annettiin nimi image.out, joka on oletuksena ladattavan firmwaren tiedostonimi FortiGate-palomuureissa. Palomuurilaitteisiin kytkettiin verkkovirta ja konsoli yhteystyöasemalta. Palomuurien oletus-firmwaren boottaus keskeytettiin konsoli-ikkunan kautta ja palomuurien kovalevyt alustettiin. Tämän jälkeen ladattiin kuvan 6 mukaisesti kannettavan tietokoneen tftp-palvelimelta viimeisin firmware palomuureihin.



Kuvio 6. FortiGate-alustus ja firmwaren asennus.

Päivitetty firmware tallennettiin palomuurien oletusimageksi bootloaderiin, jonka jälkeen kirjauduttiin konsoliyhteydellä sisään palomuurien hallintaan ja todettiin komentoriviltä laitteen nykyinen tila. Komentorivin avulla pystytään FortiGate UTM-palomuurista helposti tarkistamaan esimerkiksi laitteen firmware-versio, sarjanumero, toiminnallinen tila sekä virus- ja IPS-tietokantojen versiot.



Kuvio 7. Esimerkki FortiGate-palomuurin tilatiedoista

Virus- ja IPS-tietokantojen päivittäminen tehtiin asennettaviin palomuureihin työasemalla graafisen käyttöliittymän kautta. Oletuksena FortiGate-palomuuri tukee selainpohjaista kirjautumista https-yhteyden kautta. Palomuuria voidaan hallita myös ssh-, telnet-, http- ja snmp-protokollilla, sekä konsoliyhteydellä tai fortimanager- hallintaohjelmistolla keskitetysti. FortiGaten UTM-tietoturvapalvelimessa laitteen hallintaportit ovat vapaasti määritettävissä. Esiasennuksen viimeisessä vaiheessa määritettiin kumpaankin palomuuriin Wan-porteille Internet-liittymien julkiset IP-osoitteet, käytettävän operaattorin nimipalvelimet sekä konfiguroitiin staattinen reititys liittymien gatewayhin. Lisäksi Internet yhteyden toimivuutta varten tehtiin palomuuriin sääntö, jolla liikenne sisäverkosta ulos sallittiin ilman rajoituksia. Tämän jälkeen palomuurit asennettiin räkkikaappiin paikoilleen ja kaapeloitiin verkkoon käyttäen kategorian 6 verkkokaapeleita. Tämän jälkeen tarkistettiin Internet-yhteyden toiminnallisuus muureissa. Toimintaa testattiin lähettämällä n. 20 minuutin ajan yhtämittaisesti Icmp-viestejä liittymien gateway-osoitteisiin. Lisäksi Internet-yhteyksien nopeusprofiilit testattiin mittaamalla selainyhteydellä nopeutta speedtest.com sivuston nopeustestillä. Testauksissa päästin 0 %:in pakettihäviöön ja nopeuksissa melko lähelle liittymien teoreettisia nopeuksia.

Ennen asennuksien jatkamista jätettiin UTM-palomuurit vuorokauden ajaksi odottamaan rekisteröitymistä Fortinetn palvelimille, jotta tilatut UTM-palvelut voitaisiin ottaa käyttöön lisenssien aktivoiduttua laitteissa.

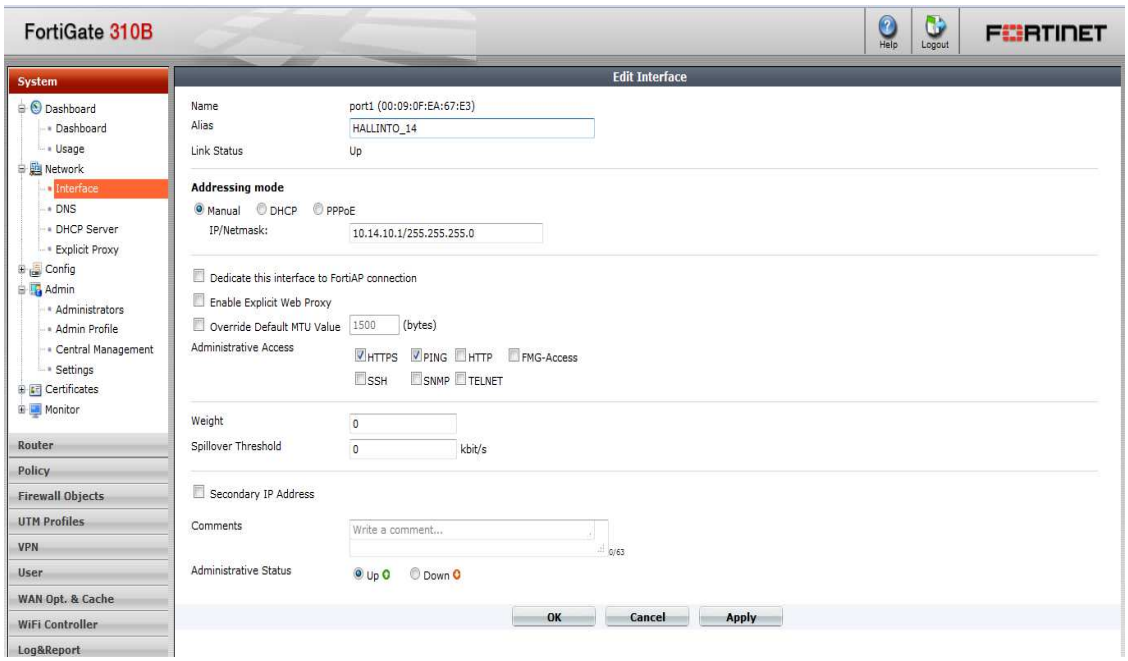
4.4 Sääntöjen määrittely

Projektin seuraavassa vaiheessa edettiin palomuurilaitteiden konfigurointiin. Laitteiden asetusten määrittely tehtiin myös tässä työvaiheessa graafisen käyttöliittymän kautta. FortiGaten UTM-laitteiden käyttöliittymää voidaan pitää asetuksien määrittelyyn kauttaaltaan helppokäyttöisenä sekä ominaisuuksiltaan riittävänä konfiguraation määrittelyyn. Graafinen käyttöliittymä ei kuitenkaan mahdollista kaikkien asetusten määrittelyjä, mutta työn tässä vaiheessa komentorivipohjaista konfigurointia ei tarvittu.

4.4.1 Verkko- ja hallinta-asetukset

Laitteiden konfiguroiminen aloitettiin määrittelemällä laitteiden hallintaa varten pääkäyttäjän (admin) salasana. Salasanaksi määritettiin tietoturvasyistä 16 merkkiä pitkä salasana, jossa käytettiin isoja ja pieniä merkkejä sekä numeroita ja erikoismerkkejä. Käytettävien salasanojen riittävä monimutkaisuus ja pituus turvaavat laiteita ulkopuolisilta dictionary- ja bruteforce-hyökkäyksiltä. Salasanoja voidaan pitää näin riittävän vahvana, jotta ne voitaisiin murtaa algoritmein kohtuullisella ajanjaksolla edes F-luokkaan luokiteltavalla hyökkäyksellä [10].

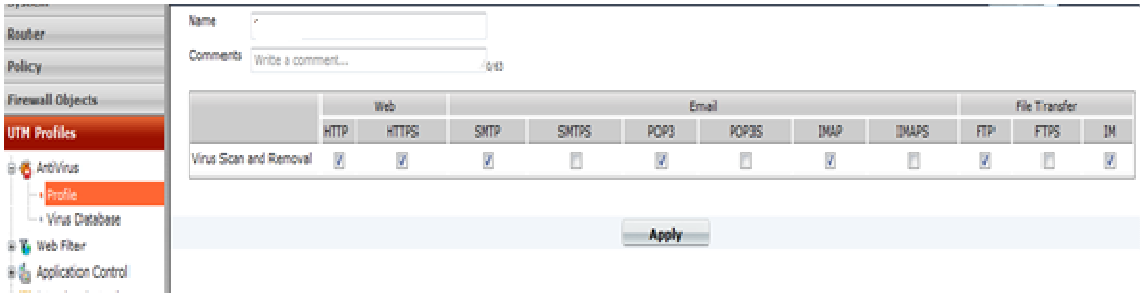
Asennetut FortiGaten UTM-palomuurit määriteltiin asennusvaiheessa port-modeen, eli jokainen laitteen fyysisistä ethernet-porteista pystytään määrittämään kukin erikseen. Konfiguraatioon määriteltiin kukin aktiiviseen käyttöön tuleva portti sallimaan hallinta yhteys https-yhteydellä. Verkon mahdollisten vikatilanteiden diagnosoinnin helpottamiseksi konfiguroitiin palomuurien fyysiset portit RFC 1122 -standardin mukaisesti vastaamaan ICMP echo (ping) -pyyntöihin [11, s. 42] ja portit nimettiin vastaamaan verkkokytkentöjä. Käyttämättömät portit asetettiin hallinnollisesti suljettuun tilaan (administratively down), jotta näiden porttien kautta ei pystytä fyysisellä kaapeliyhteydellä saavuttamaan yhteyttä palomuureihin tai sisäverkkoon. Kuviossa 8 on esimerkki ethernet-portin konfiguroinnista graafisen käyttöliittymän kautta.



Kuvio 8. FortiGate-310B-ethernet-portin asetukset

4.4.2 Antivirusprofiili

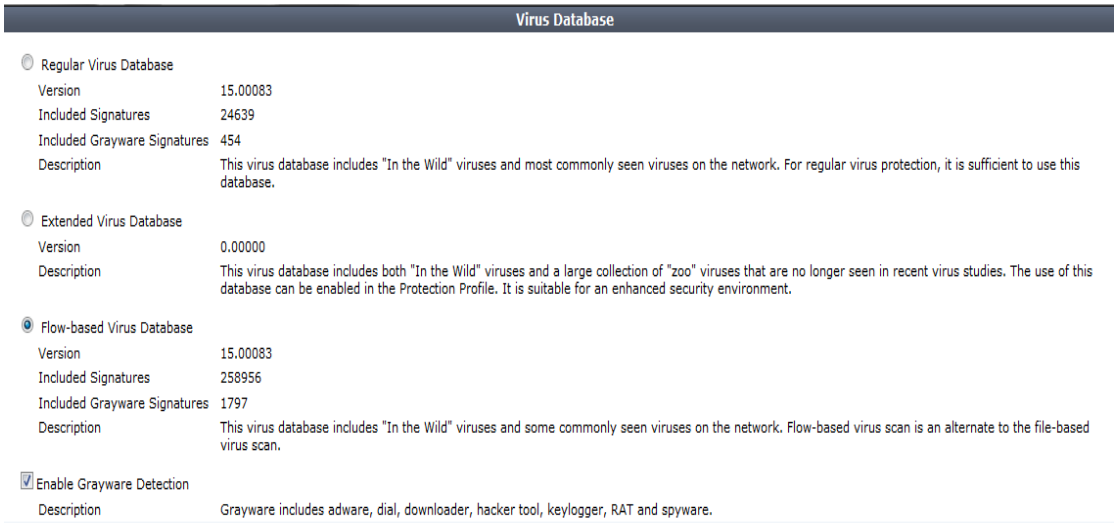
Projektin tässä vaiheessa edettiin määrittelemään käyttöön tulevia tietoturvapalvelimien UTM-ominaisuuksia. Konfiguraatioiden määrittely aloitettiin määrittelemällä molemmille palomuureille käyttöön tulevat antivirusprofiilit. Profiilien konfiguraatioissa luotiin palomuuriin asiakasta varten oma profiili, jossa määritettiin suunnitelman pohjalta, minkä tyyppinen liikenne verkkoliikenteestä tutkitaan. Lisäksi määritettiin käytettävä virustietokanta. Profiilin määrittelyssä päädyttiin hyödyntämään FortiGaten mahdollisuutta tutkia verkkoliikenteestä mahdolliset virukset normaalin http liikenteen lisäksi myös https-liikenteestä. Lisäksi myös viruksia useasti levittävä sähköpostiliikenne asetettiin tutkittavasti kaikista yleisistä sähköpostiprotokollista, joita asiakasverkossa esiintyy. Tässä tapauksessa profiiliin määritettiin pop-, imap- ja smtp-suodatus päälle. SSL-suojattua sähköpostiliikennettä ei asiakkaan verkossa ole käytössä, joten tämä jätettiin virustarkistuksen profiilin ulkopuolelle. Lisäksi myös FTP- ja pikaviestimien liikenne asetettiin profiilin konfiguraatiossa tutkittavien listalle.



Kuvio 9. FortiGate 310B: Hallinto- ja opetusverkon antivirusprofiili

Palvelinverkon suojaksi asennetussa FortiGate-800 UTM-tietoturvapalvelimella hyödynnettiin virustutkan ominaisuutta eristää saastunut laite verkosta, mikäli virus havaitaan liikenteestä. Antivirusprofiilin määrittelyssä palvelinverkon puolella huomioitiin mahdollisuus lisätä myöhemmin verkkoratkaisuun esimerkiksi FortiGaten analysaattori, jonne esim. virus voitaisiin eristää karanteeniin. Karanteeni olisi ollut mahdollista määrittää myös paikalliselle laitteen kovalevylle, mutta tätä ei nähty tarpeelliseksi vaan optiota erilliselle analysaattorille pidettiin järkevämpänä ratkaisuna.

Konfiguraatiossa määritettiin antivirusprofiileissa myös verkkoliikenteeseen grayware-suodatus. Tällä suodatukselle liikenteestä pyritään löytämään työasemille mahdollisesti haitalliset ohjelmat, kuten vakoilu- ja haittaohjelmat sekä erinäiset hakkerointityökalut ja niin sanotut keyloggerit. Palomuurien määrittelyissä opetus- ja hallintoverkoille asetettiin virusskannaus suoritettavaksi liikenteestä lennosta, jolloin liikenteestä tutkitaan puskuroitua mallia enemmän edellä mainittuja haittaohjelmia. Lennosta tutkittuna myös palomuurin läpäisykyky liikenteelle on parempi (350 Mbs) verrattuna puskuroituun (160 Mbs) skannaukseen [12]. Haittapuolena tässä voidaan pitää sitä, että tutkittavassa paketissa ei voida palata enää tutkimaan jo skannattua osiota paketista.



Kuvio 10. FortiGate 310B: Käytettävän virustietokannan määrittely

4.4.3 IPS

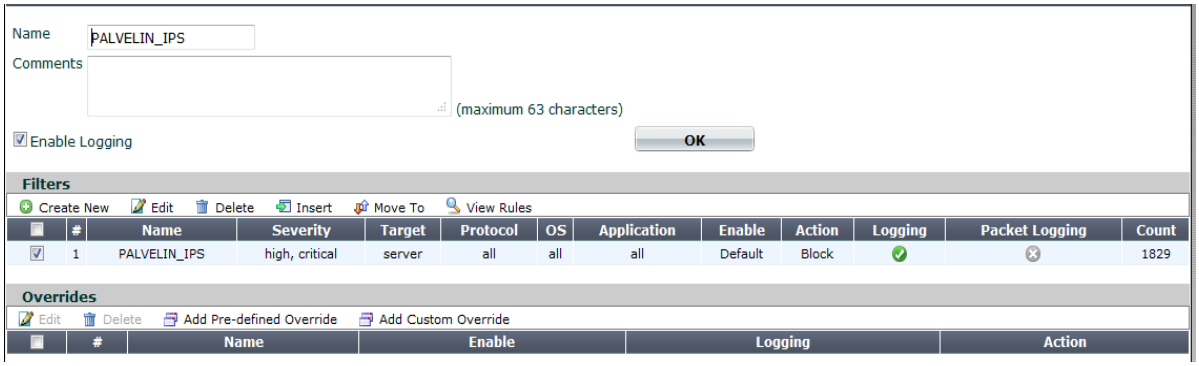
FortiGaten UTM-laitteissa on mahdollista käyttää valmiita IPS-sensoriprofiileja. Näiden profiilien avulla voidaan nopeasti ottaa käyttöön valmiita sensori malleja, joilla voidaan suojautua ainoastaan kriittisiltä Windows-työasemiin kohdistuvilta hyökkäyksiltä. Palomuurien määrittelyssä luotiin kuitenkin omat sensorit, jotta sensorien konfiguraatio saatiin vastaamaan täsmällisemmin suojattavien verkkolaitteiden ja työasemien ominaisuuksia.

Opetus- ja hallintoverkolle luotiin uusi sensori profiili, johon määritettiin uusi IPS-suodatin. Suodattimen toiminta rajattiin tutkimaan verkkoliikenteestä kriittisen ja korkean tietoturvariskin luokituksen mukaisia hyökkäyksiä. Käytettävän IPS-suodattimen toiminta määritettiin toimimaan ns. signature based -muodossa. Tällöin suodattimen toiminta perustuu Fortinetin tietoturvalaboratorion tietokantaan, jossa signaturet sisältävät tiedon tunnetusta tietoturvauhkan aiheuttavasta haittakoodista. Haittakoodin mukaisia esiintymiä etsitään verkkoliikenteen paketeista. Signaturet sisältävät oletustoimintamallin mikäli tämän tyyppinen uhkatekijä kohdataan verkkoliikenteestä. FortiGate-palomuureissa signaturet sisältävät muun muassa tiedon, onko kyseinen signature aktiivinen ja pudotetaanko signaturen mukainen liikenne vai sallitaanko se. Tässä projektissa määritettiin IPS-suodatin hyväksymään tietokannan signaturejen oletustila aktiivisuuden suhteen, mutta konfiguraatio suodattimessa muutettiin niin, että mikäli liikenteestä havaitaan signaturen laukaiseva hälytys, niin paketit hylätään ja lokitietoi-

hin kirjataan hälytys ja tiedot tapahtumasta. Lisäksi hälytyksen aiheuttaneet hyökkääjän ja kohteen IP-osoitteet asetettiin automaattisesti vuodeksi karanteeniin. Karanteeniin asetetut osoitteet voidaan sallia verkkoliikenteessä uudestaan käsin graafisen käyttöliittymän tai komentorivin kautta. Tällöin kyseinen IP-osoite poistetaan karanteenista. Konfiguroidun suodattimen avulla suojattiin opetus ja hallintotoimen verkko yhteensä kuvion 11 mukaisesti yli 2500 tunnetulta verkkohyökkäykseltä.

Kuvio 11. FortiGate-310B IPS -suodattimen määrittely.

Palvelinverkon puolella myös FortiGate-800 UTM-palomuurille konfiguroitiin oma IPS-sensori ja suodatin. Palvelinverkon suodattimen konfiguraation erona aiemmin määritettyyn opetus- ja hallintoverkon suojaavaan IPS-suodattimeen oli, että määrittelyssä valittiin suodattimeen vain signaturet, jotka kohdistuvat palvelimiin. Palvelimien käyttöjärjestelmistä suojattiin kaiken tyyppiset järjestelmät, sillä verkossa toimii pääsääntöisesti Windows- ja linux-palvelimia, mutta Macintosh-järjestelmien mahdollisuus tulevaisuudessa nähtiin myös mahdollisena ja tämän vuoksi myös näihin järjestelmiin kohdistuvat hyökkäykset otettiin suodattimeen mukaan. Kuviossa 12 nähdään yhteenvetonäkymä IPS-sensorin suodattimesta.



Kuvio 12. FortiGate-800 palvelinverkon IPS-sensorin suodatin.

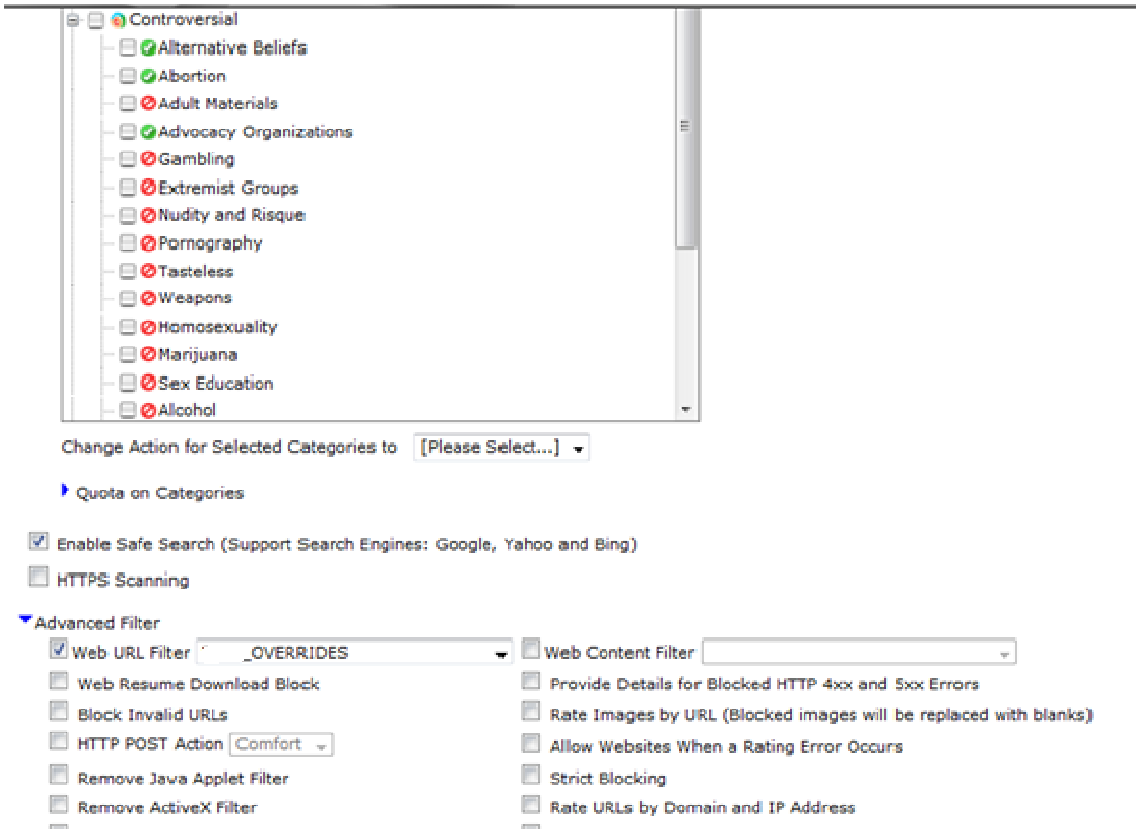
FortiGate-800-muurilla ajettavassa firmware-versiossa erona oli, että hyökkääjän ja kohteen IP-osoitteet pystyttiin asettamaan karanteeniin pysyvästi, kun taas 310B-mallin ohjelmisto mahdollisti enintään vuoden mittaisen karanteeniin. Lisäksi FortiGate-800-mallissa olisi ollut mahdollista myös hyökkäyshälytyksen aiheuttaneen paketin sisällön tallentaminen lokiin. Ominaisuuden todettiin kuitenkin tässä vaiheessa olevan epäolennainen ja ominaisuuden käyttöönotto nähtiin järkeväksi, mikäli ulkoinen analysaattori lisättäisiin käyttöön. Kuten opetus- ja hallintoverkon suodattimessa, myös palvelinverkon hälytykset kuitenkin konfiguroitiin kirjattavaksi UTM-lokiin, jotta hälytyksistä jäisi tarkasteltavaksi merkintä palomuuriin, josta tieto hyökkäyksen aiheuttajasta ja kohteesta saataisiin selvitettyä.

4.4.4 Verkkosisällön suodatus ja DLP

Palomuurien konfiguraatioiden määrittelyssä edettiin vaiheeseen, jossa tultaisiin määrittämään selattavalle www-sisällölle suodatus. Suunnitelmien mukaisesti verkossa tultaisiin sisällön suodatus kohdistamaan opetusverkon puolelle, jossa käyttäjinä on opiskelijat. Hallintotoimen verkoille ei suodatuksen tarvetta tässä vaiheessa nähty, sillä verkon käyttäjäryhmää pidettiin uhkana verkolle melko pienenä ja käyttäjäkuntaa melko valveutuneina Internetin sisällön uhkista. Suodatuksen avulla haluttiin hallita verkkoon kohdistuvaa tietoturvaauhkaa, joka aiheutuisi ns. hallitsemattomasta verkon käytöstä.

FortiGate-310B palomuuriin luotiin uusi web-suodatinprofiili, johon määritettiin toiminta tietyn tyyppistä sisältöä sisältäville sivustoille kategorioittain. Web-sivuille on Fortinetin toiminnasta asetettu sisällön perusteella kategoria, joka palautetaan tietokannasta haettavalle URL:lle. Sivuston tyypin määrittely tapahtuu pilvipalvelu-ratkaisuna eikä lop-

pukäyttäjä huomaa normaalissa selauksessa kategorialuokituksen hausta aiheutuvaa viivettä. Web-filterissä FortiGaten palomuuri joko asetetaan sallimaan tai estämään liikenne kategorian mukaisille sivulle. Tässä projektissa päädyttiin oppilasverkolta haettavasta www-sisällöstä sallimaan niin sanotun hyvän tavan mukaiset sivustot. Suodattimesta konfiguroitiin estettäväksi pornografiaa, väkivaltaa, piratismia, huumeita ja aseita sisältävät sivustot. Myös uhkapelaamisen mahdollistavat sivustot ja peer-2-peer-ohjelmistoja käsittelevät sivut asetettiin suodattimessa estetyiksi. Lisäksi suodattimesta asetettiin SafeSearch-ominaisuus käyttöön. Tämän ominaisuuden avulla yleisimpien hakukoneiden kuten esim. Googlen tai Yahoon antamien hakutulosten sisällöstä pystytään suodattamaan haitalliset tulokset, kuvat ja tekstit pois. Lisäksi suodattimeen asetettiin käyttöön oma URL-suodatin, johon pystytään määrittämään suoraan sivustojen osoitteita ja määrittämään sivustot suoraan estetyiksi tai sallituiksi ilman, että sivustolle haetaan luokittelua Fortinetin tietokannoista. Kuviossa 13 on esimerkki, kuinka FortiGaten web-filterin määrittely on tehty graafisen käyttöliittymän avulla.



Kuvio 13. FortiGate web -suodattimen määrittely.

FortiGaten web-filterin ominaisuuksista olisi ollut myös mahdollista ottaa käyttöön ominaisuudet, joilla www-sisällöstä olisi voitu estää esim. Java-, ActiveX- ja Cookie-(eväste) ominaisuudet. Kuvion 13 mukaisesti myös sivustojen lomakkeille, kuville, osoitteille voidaan asettaa vaateita luokituksen suhteen. Näitä ominaisuuksia ei kuitenkaan otettu käyttöön, sillä näiden ominaisuuksein käyttö aiheuttaa usein epäedullisia ominaisuuksia sivustojen visuaalisiin ulkoasuihin. Myös tässä tapauksessa haluttiin tietoturvasta tinkiä, jotta web-sisällön käyttäjäystävällisyys saatiin toteutettua.

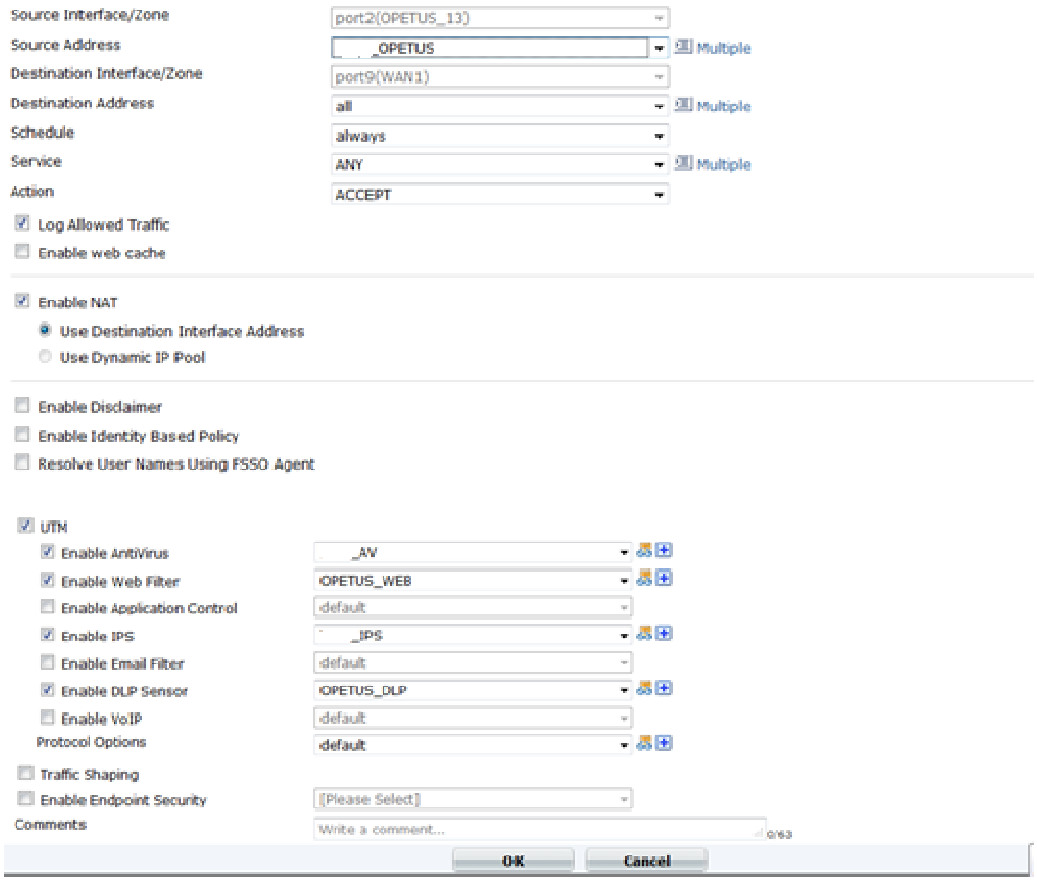
Opetusverkkoon konfiguroitiin myös yksinkertainen DLP-suodatin, jolla estettiin verkosta yleisimpien koodia suorittavien ohjelmatiedostomuotojen lataaminen. Tämän ominaisuuden avulla pystytään ehkäisemään suurilta osin tietoturvauhka, joka verkolle koituu verkon käyttäjän toimista. Usein verkosta ladataan ohjelmia, joiden asennuspakettien todellisesta sisällöstä ei ole mitään takeita. Määritetyn DLP-suodattimen avulla estettiin tällaisten tiedostojen tahallinen ja tahaton lataaminen verkosta ja verkkoon. Lisäksi suodattimen avulla helpotettiin työasemien ylläpitoa, kun ylläpidon ulkopuolella olevien verkkoselaimien lataaminen pystyttiin estämään. Kuviossa 14 on esimerkki DLP-suodattimen tiedostofiltterin määrittelystä.

Kuvio 14. FortiGate DLP -tiedostosuodattimen määrittely.

4.4.5 Säännöstö ja virtual IP

Projektissa edettiin vaiheeseen, jossa asennettuihin UTM-palomuureihin alettiin laatia varsinaista palomuurisäännöstöä. Säännöstön avulla voidaan hallita verkon liikennettä käyttäen lähde- tai kohdeporttia ja osoitteita. Lisäksi liikenteen salliminen tai estäminen voidaan rajata haluttuihin protokolliin. Määriteltyihin sääntöihin voidaan jokaiseen lisäksi erikseen määrittää käyttöön haluttavat UTM-ominaisuudet ja profiilit. Palomuurisään-

töjen luontia varten luotiin palomuureihin objektit, joilla voitiin määrittää IP osoitteille, IP aliverkoille tai verkkolaitteille FQDN:n (absoluuttinen laitenimi) perusteella oma kuvaava nimi. Luotaviin objekteihin voidaan lisäksi myös määrittää, mihin palomuuriin fyysiseen porttiin käytettävä osoite tai aliverkko on sidottu. Kuviossa 15 on esimerkki palomuurisäännön määrittelystä. Säännön määrittelyssä on hyödynnetty luotuja palomuuriobjekteja.



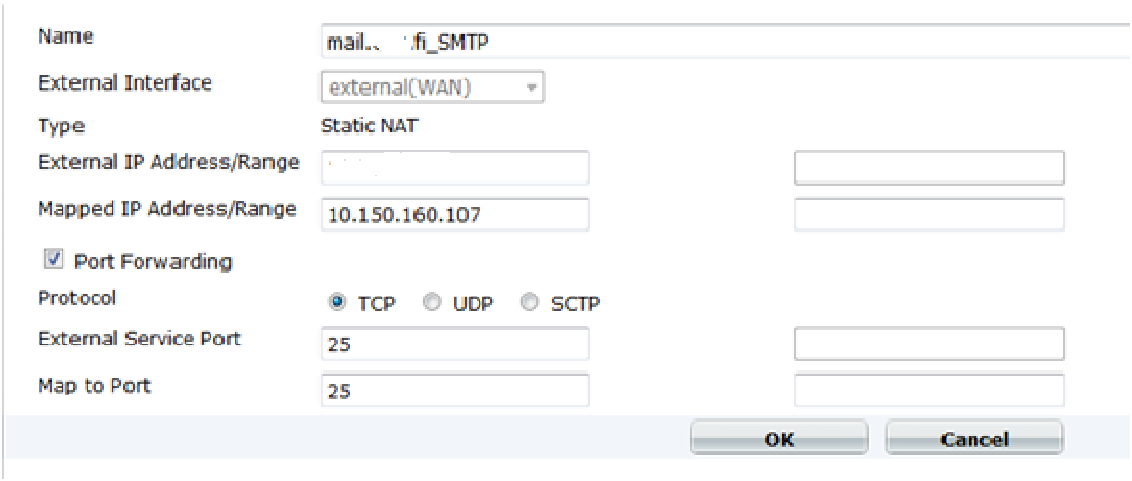
Kuvio 15. FortiGate-palomuurisäännön määrittely.

Säännöstössä normaalissa pienemmissä verkkoympäristöissä usein riittää, että säännöstössä sallitaan liikenne ulospäin. Kuvion 15 sääntö on yleinen sääntö, jota sovelletaan yleisesti ulospäin suuntautuvaan liikenteeseen. Säännöstöön kuitenkin jouduttiin tekemään opetustoimen verkolle useampia sääntöjä, joihin sovellettiin harvennetusti UTM-ominaisuuksia. Syynä poikkeuksille oli esimerkiksi WSUS- ja F-Secure-palvelimina toimivien työasemien tarve ohittaa muun muassa DLP-suodatus. Lisäksi eräillä opetukseen liittyvillä Internet-sivustoilla web-suodattimen toiminta aiheutti rajoitteita sivuston oikealle toiminnalle, jolloin myös näille www-palvelimille suuntautuva liikenne määritel-

tiin sallituksi, mutta liikenteelle asetettiin kuitenkin suoritettavaksi palomuurissa virustarkistus.

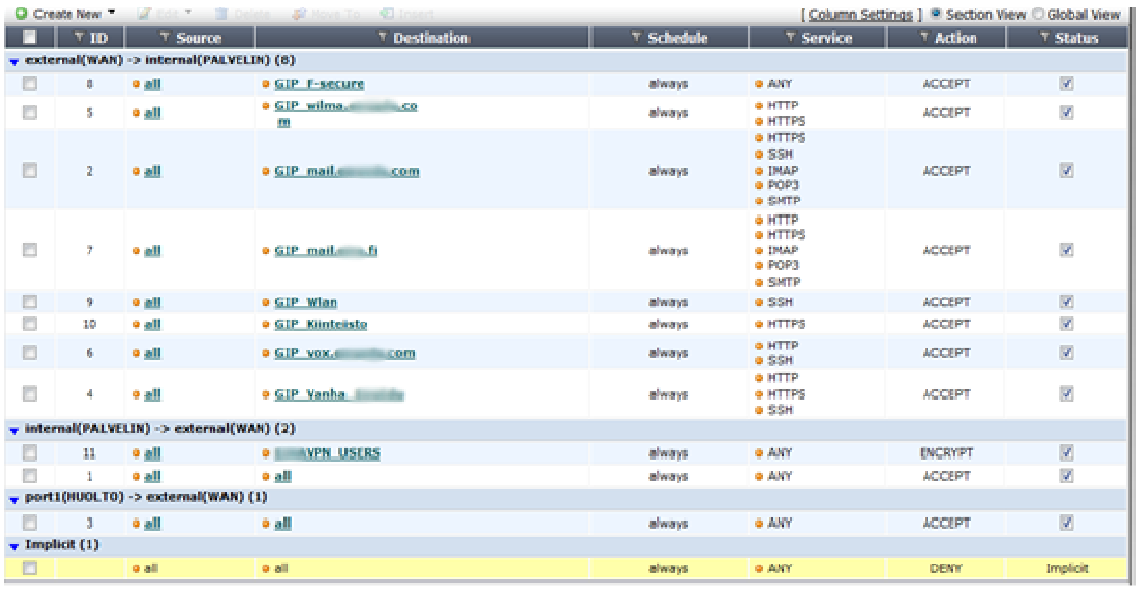
Varsinaista säännöstön määrittelyä jouduttiin projektissa pohtimaan enemmän palvelinverkon suojaavassa FortiGate-800-palomuurissa. Palvelinverkkoon kuuluvien opetus- ja sähköpostipalvelimien saatavuus julkisiin verkkoihin toteutettiin tässä projektissa hyödyntämällä FortiGate-palomuurien virtual IP -ominaisuutta. Virtual IP:n avulla voidaan tehdä staattisia portti- ja osoitekäännöksiä FortiGate -palomuureissa. Porttiohjauksia voidaan määrittää TCP-, UDP- ja SCTP-protokollille. Tässä projektissa jokaiselle palvelimelle oli käytettävissä julkinen IP-osoite, jolloin ohjaus konfiguroitiin tehtäväksi palomuurin Wan-portilta sisäverkkoon. Ohjauksia varten Wan-portille konfiguroitiin varsinaisen liittymän IP-osoitteen lisäksi sekundäärisiksi IP-osoitteiksi kaikkien palvelinten julkiset IP-osoitteet.

Virtual IP tarkoittaa FortiGaten omassa terminologiassa palomuureissa tehtävää kohdeosoitekäännöstä (destination NAT), eikä tätä tule sekoittaa esimerkiksi HSRP:ssä (Hot Standy Router Protocol) käytettävään Virtual IP:hen. Eri laitevalmistajan käyttävät usein yleisesti tunnettuja termejä omissa prosesseissaan eri tarkoituksiin. Projektin asennuksissa Virtual IP -määrittelyt konfiguroitiin palvelinverkon palomuurille niin, että julkisen IP-osoitteen viimeinen oktetti säilytettiin myös selkeyden vuoksi sisäverkon IP-osoitteen viimeisenä oktettina. Myös ohjattava portti säilytettiin samana. Jokaista palvelinta varten luotiin ensin halutut portti- ja osoiteohjaukset. Tämän jälkeen hyödynnettiin FortiGaten virtual group -ominaisuutta, jolla usempi virtual IP voidaan liittää saman ryhmän alle. Luotuja virtuaalisia osoiteryhmiä voidaan käyttää suoraan luotaessa palomuuriin liikennettä kontrolloitavia sääntöjä. Virtuaalisia IP-ohjauksia konfiguraation määriteltiin yhteensä 21 kpl ja virtuaalisia osoiteryhmiä yhteensä 8. Kuvassa 16 on esimerkki virtuaalisen IP:n määrittelystä FortiGate-palomuurissa.



Kuvio 16. FortiGate-800 Virtual IP -määrittely.

Lopuksi FortiGate-800-palomuuriin määriteltiin varsinaiset palomuurisäännöt. Liikenteen kontrollointi tapahtuu sääntöjen avulla pääsylistojen toimintaan verrattavalla tavalla. Paketin saapuessa muurin porttiin aletaan säännöstöä käydä läpi alusta loppuun. Jos paketti ei kohdistu mihinkään sääntöön, joutuu se hylätyksi lopussa olevan implisiittisen kieltolausekkeen johdosta. Kuviossa 17 on esitelty yhteenveto määritetyistä säännöistä FortiGate-800-palomuurista, jolla siis suojattiin organisaation palvelinverkko.

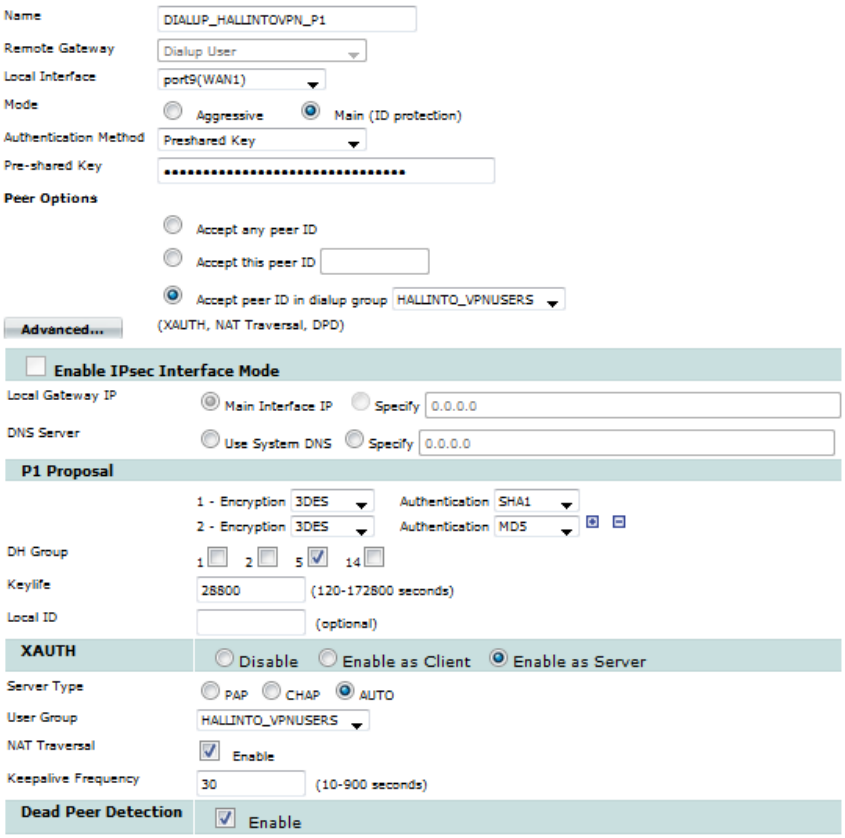


Kuvio 17. FortiGate-palomuurin säännöstön yhteenveto.

4.4.6 VPN-yhteydet

Asennusten edetessä täsmentyi projektin suunnitelmat tarkemmiksi, ja myös etäyhteyksien tarve nähtiin tarpeellisena. FortiGaten palomuureissa on mahdollista toteuttaa VPN-yhteydet joko IPSec VPN:llä tai SSL-VPN:llä. VPN-yhteydet voidaan tehdä joko reitteihin tai palomuurisääntöihin perustuen. Reitteihin perustuvissa VPN-yhteyksissä hyödynnetään FortiGaten virtuaalista porttia, jonka kautta tunneloitu liikenne reititetään. Tässä projektissa päädyttiin kuitenkin käyttämään sääntöpohjaista tunneloitua IPsec VPN:ää, jolloin palomuurin säännöstö saadaan pidettyä yksinkertaisempana. Sääntöpohjaisesti toteutetussa VPN-yhteydessä tunnelointiin tarvitaan vain yksi sääntö sisäverkosta ulkoverkkoon.

Tämän projektin yhteydessä päädyttiin konfiguroimaan palomuureihin IPsec VPN-yhteyksiä varten jokaiselle etäyhteyden käyttäjälle omat tunnukset. Projektissa haluttiin hyödyntää palomuurin XAuth (extended authentication) -ominaisuus ja minimoida tältä osin muutosten määrä loppukäyttäjien etäyhteyksien osalta, sekä lisätä verkon tietoturvaa vahvistamalla käyttäjien autentikointia. FortiGaten palomuurien avulla olisi voitu toteuttaa IPSec VPN-autentikoinnin integraatio suoraan esimerkiksi Windows-palvelimen aktiivihakemistoon tai erilliseen Radius-palvelimeen. Asennetut palomuurit tukevat myös VPN-autentikointia käyttäen RSA X.509 -turvasertifikaatteja. Etäyhteyksien konfiguroinnissa määritettiin VPN-yhteyden muodostamisen molempiin vaiheisiin käytettäväksi kevyet, mutta riittävän turvalliset algoritmit. FortiGaten palomuurit tarjoavat hash-algoritmiksi (datan tiiviste) jopa 512 bittistä SHA:ta (kryptografinen tiivistefunktio), mutta tämän tason suojauksella ei voida hyödyntää FortiGaten mikropiirien kiihdytystä, joka aiheuttaa suorituskyvyssä jopa huomattavaa laskua [8, s. 1331]. Kuviossa 18 on esimerkki IPsec VPN -yhteyden ensimmäisen vaiheen määrittelystä FortiGate-palomuurissa.



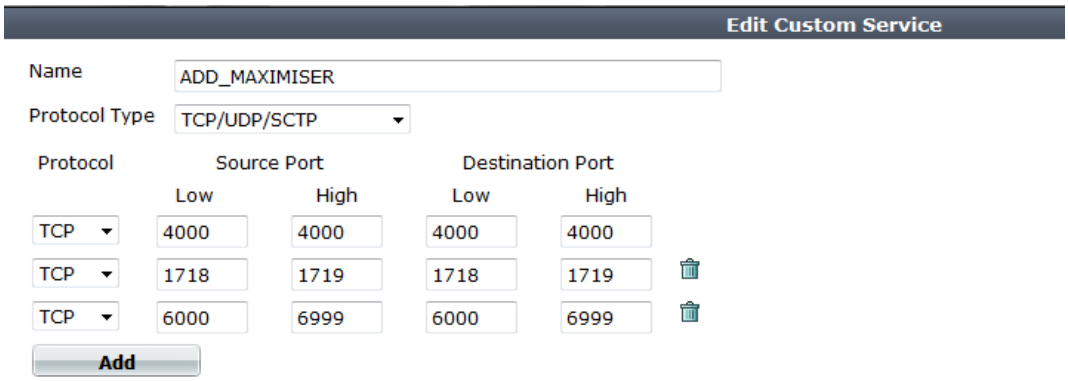
Kuvio 18. FortiGate IPsec VPN:n -määrittely.

Loppukäyttäjien etäyhteyden muodostamiseen käytettävä asiakasohjelmisto vaihdettiin Ciscon ohjelmistosta Fortinetin omaksi FortiClient-ohjelmaksi. Asennettaviin palomuureihin ei asennuksien tässä vaiheessa konfiguraation osalta otettu kantaa mahdollisiin myöhempiin site-to-site (toimipaikkojen välinen) VPN -ratkaisuihin.

4.4.7 VoIP-integraation valmistelu

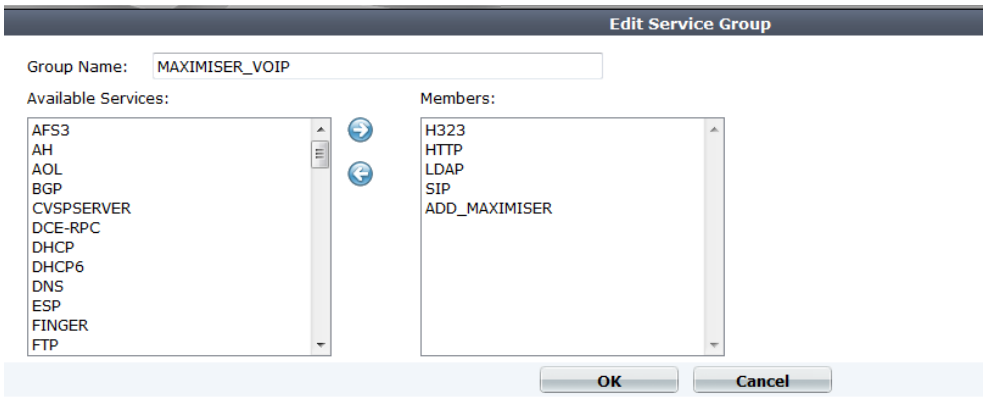
Projektin viimeisessä vaiheessa määritettiin FortiGate-800-palomuurin konfiguraatioon tarvittavat esivalmistelut myöhemmässä vaiheessa käyttöönotettavaa VoIP-ratkaisua varten. Projektin tässä vaiheessa VoIP-järjestelmää rakennettiin ja sen käyttöä testattiin erillisen operaattori-yhteyden kautta erillisenä varsinaisesta yritysverkosta. Käyttöön tulevia laitteita varten tuli FortiGaten palomuureihin lisätä tarvittavat esimääritetyt protokollat, joita VoIP-laitteisto tulisi käyttämään. Tätä varten palomuuriin luotiin uusi palveluprotokolla, johon määritettiin tarvittavat TCP-protokollaportit, joita esimäärite-

tyistä protokollista ei löytynyt. Kuviossa 19 on esimerkki asennuksissa esimääritetyn protokollan lisäämisestä palomuurin konfiguraatioon.



Kuvio 19. Protokollan määrittely FortiGate UTM -palomuurissa.

Tarvittavien protokollamäärittelyjen jälkeen luotiin vielä oma protokollaryhmä, johon koottiin kaikki laitteiston tarvitsemat protokollat. Ryhmämäärittelyn avulla pystytään VoIP-järjestelmän käyttöönotossa helposti määrittämään palomuurisäännöstöön tällä tavoin yhden säännön avulla sallittavat yhteydet puheliikenteen kannalta. Määritelty protokollaryhmä on esitelty kuviossa 20.



Kuvio 20. Protokollaryhmän määrittely FortiGate-palomuurissa.

Liikenteen priorisointia varten ei palomuuriin tehty määrittelyjä valmiiksi projektin tässä vaiheessa, vaan näiden asioiden konfiguraatio päätettiin jättää VoIP-järjestelmän käyttöönottohetkeen. Tällöin voitaisiin testikäytön perusteella kerätystä datasta analysoida tarvittavat liikenteen priorisointitarpeet. FortiGaten palomuureissa on tarjolla valmiita

malleja liikenteen priorisointiin, mutta palomuurien määrittelyt tullaan tekemään integraation yhteydessä vastaamaan todellista verkon käyttöä VoIP-liikenteen osalta.

4.5 Kohdatut ongelmat ja kehityskohteet

Projekti onnistui kokonaisvaltaisesti erinomaisesti, vaikka pieniä vastoinkäymisiä kohdattiin useampaan otteeseen. Ensimmäisen ongelman aiheutti Internet-operaattorin tuen aikataulutuksen epäonnistuminen. Aiemmin käytössä ollut julkinen IP-aliverkko, jossa palvelimien käyttämät osoitteet olivat, tuli suunnitelman mukaisesti reitittää operaattorin toimesta kiinteistöön asennettuun uuteen kuituliittymään. Operaattorin kankeasta toiminnasta tässä suhteessa koettiin projektissa alkuvaiheessa turha viivästys.

Ensimmäinen suunnitelmallinen ongelma kohdattiin Exindan kaistankiihdyttimen kanssa. Ongelmaksi muodostui fyysisten porttien riittämättömyys. Käytetty kaistankiihdytin ei ominaisuuksiltaan pysty purkamaan kahden sisääntulon liikennettä yhdelle ulostulolle. Ongelma ratkaistiin lisäämällä kaistankiihdyttimeen yksi verkkokortti lisää, jolloin liikenne saatiin kiihdytettyä molemmille palomuureille erikseen.

Myös FortiGaten palomuureissa kohdattiin konfiguraation osalta ongelmia. Ensimmäisenä ongelmana havaittiin FortiGaten www-sisällönsuodatuksen suorittamisen puskuroimattomana aiheuttavan Flash-sovellusten kanssa ongelmia näiden latautumisessa. Ongelma korjaantui, kun määritettiin, että suodatus tehdään puskuroituna.

Etäyhteyksien määrittelyssä oli tarkoitus alun perin määritellä etäyhteydet erillisillä palomuurisäännöillä erikseen opetus- ja hallintotoimen verkoille. FortiGaten säännöstö kuitenkin ohjasi saapuvan tunneloidun liikenteen aina hallintoverkon IPsec VPN -säännön mukaisesti, eikä etäyhteyttä suoraan opetustoimen verkolle saatu muodostettua. Ongelman aiheuttajalle ei löydetty suoranaista selitystä ja asia siirrettiin Fortinetin tukiportaalin selvitettäväksi. Hallintotoimen verkkoon asennettiin asiakkaan toimesta työasema, johon voitiin ottaa useita samanaikaisia etätyöpöytäyhteyksiä.

Asennusten valmistumisen jälkeen koettiin pian ongelma, joka johtui operaattorin toimittaman reitittimen vikaantumisesta. Ongelma ratkaistiin kierrättämällä vikaantuneen

liittymän palomuurin liikenne toisen asennetun palomuurin läpi, kunnes operaattori vaihtoi laitteen toimivaan.

Ylitsepääsemättömiä ongelmia ei projektissa lopulta tullut vastaan, mutta kompromisseja jouduttiin tekemään palomuurien osalta niin UTM-ominaisuuksissa kuin etäyhteyksien saralla. Aikataulullisesti projektin etenemisessä kohdatut ongelmat aiheuttivat viivästyksiä, mutta väljän aikataulun johdosta eivät viivästykset aiheuttaneet ongelmia verkon käyttöönotolle, ja projekti valmistui ajallaan.

Asennettua tietoturvaratkaisua pystyttäisiin edelleen kehittämään ja ominaisuuksia laajentamaan. Verkkolaitteiden kahdentamisella ja aktiivi-passiivi tilan määrittelyn avulla pystyttäisiin suojautumaan laitteiden mahdolliselta vikaantumiselta. FortiGaten tietoturvaominaisuuksista myös sovellushallinnan käyttöönottoa kannattaisi harkita, jolloin voitaisiin parantaa verkon tietoturvaa organisaation sisäisiltä tietoturvariskeiltä. Mikäli liikenne sallittaisiin vain laitteilta, joiden päivitykset ja virustorjuntaohjelmistojen ajantasaisuus olisi kunnossa, pystyttäisiin välttymään osaltaan näistä seikoista johtuvista uhkista.

4.6 Ylläpito

ICT-House Group Oy tarjoaa asentamilleen FortiGaten UTM-tietoturvalaitteille kuukausittaisen puolentunnin ylläpidon lisenssien voimassaoloaikana. Myös tämän projektin asennusten jälkeen oli aika siirtyä monitoroimaan laitteiden toimintaa ja seurata kuukausittaisella tasolla palomuurien lokitietoja. Kuukausittaisen ylläpidon aikana palomuureista tarkistetaan laitteiden tila (prosessorin- ja muistinkäyttö, sekä lisenssien voimassaolo), yhteydet FortiGuardin palvelimiin, konfiguraatio varmuuskopioidaan sekä liikenteen statistiikka sekä havaitut UTM–hälytykset tarkistetaan ja raportoidaan. Lisäksi tarvittaessa palomuurien firmware päivitetään.

Asennusten jälkeisinä kuukausina havaittiin pikaisesti, kuinka paljon FortiGaten palomuurien avulla pystyttiin suodattamaan jo verkon reunalla viruksia. Kuukausittaiset lukemat olivat alkuun melko suuria, mutta saavutettuna etuna pystyttiin pienentämään keskitetyn F-secure-palvelimen kuormaa sekä estämään mahdollisia viruksia, joita F-secure ei välttämättä olisi havainnut. Keskiarvollisesti palvelinverkon palomuuri suodattaa verkkoliikenteestä yli 2000 virusta kuukausittain. DLP-sensorin avulla estettiin pal-

jon organisaation verkkoon kuulumattomien ohjelmien latauksia. Ylläpidollisesti seurattuna opetus ja hallintoverkon palomuuri estää kuukausittain noin 350 latausta. Opetusverkolle asetetulla tiukalla web-suodatuksella on kuukausittain estetty yli 8000 verkkosivuston latausta. IPS-suodattimella on molemmissa asetetuissa palomuureissa estetty 3-5 hyökkäystä kuukausitasolla. Vahvana poikkeuksena kuitenkin oli joulukuu 2011, jolloin palvelinverkkoon suuntautuneesta liikenteestä estettiin 53 verkkohyökkäystä.

5 Päätelmä

Tietoturva kehittyy huimaa vauhtia, mutta silti uhkien kehitys on vieläkin voimakkaampaa. Tietoturvatalojen on yhä haastavampaa pysyä mukana uhkien torjunnassa ja tunnettujen uhkien leviämisen estämisessä. Käyttäjä on aina tietoturvan suurin uhka. Käyttäjien valistamiseen ja kouluttamiseen uhrataan liian vähän resursseja. Tämä korostaa verkon ylläpitäjien roolia tietoturvan kehittämisprosessissa. Oikeiden työkalujen ja menetelmien löytäminen ei aina ole helppoa, mutta tähän haasteeseen pyritään nykyään vastaamaan tietoturvapalveluiden keskittämisellä.

Nykyaikainen uuden sukupolven palomuuri laitteisto tarjoaa kattavan kokoelman työkaluja verkon kokonaisvaltaiseen suojaamiseen. Ratkaisuna UTM-palomuurit ovat helppoja ja kustannustehokkaita, mutta ennen kaikkea niiden tietoturvaa edistävää vaikutusta voidaan pitää kiistämättömänä. Yksittäisen työaseman virusturvaohjelmiston tarvetta UTM-laitteilla ei voida poistaa. Palomuuri suojaa loppukäyttäjiä vain, kun he ovat verkossa, joka on suojattu palomuurilla.

Tässä projektissa perehdyttiin UTM-palomuurien yleisimmin käytettyihin ominaisuuksiin ja niiden toimintaan. Lisäksi työssä esiteltiin yleisesti FortiGaten UTM-palomuurilaitteiden konfiguroimista graafisen käyttöliittymän kautta. Projektista rajattiin ulkopuolelle toiminnallisuudet, jotka voidaan konfiguroida FortiGate UTM-laitteisiin ainoastaan CLI:n kautta. Lisäksi projektissa esiteltiin mahdollisuudet verkon jatkokehittämiselle ja verkkoliikenteen syvemmälle analysoinnille, mutta tässä työssä fokus asetettiin kokonaisvaltaisesti projektissa toteutettuun palomuuriratkaisuun.

Projektin lopputuloksena asiakkaalle toteutettiin verkkoympäristön osa-alue, jossa sekä tietoturva että suorituskyky kohtaavat. Rakennetulla UTM-laiteratkaisulla pystyttiin tuomaan asiakkaan verkkoon lisää hallittavuutta. Verkkoliikenteen säätely ja tarkkailu saatiin oman hallinnan alaiseksi sekä riippuvuus operaattorien palveluihin purettua. Ennen kaikkea projektissa oltiin tyytyväisiä asiakkaan puolelta siihen, että verkon laitteet on suojattu projektin myötä kahden eri valmistajan virustorjunnalla sekä hallittavuuden ja vianselvityksen helpottumiseen suorien kontaktien myötä tukipalveluihin. Rakennettua verkkoympäristöä voidaan kokonaisuudessaan pitää edistyksellisenä ja vertailukelpoisena esimerkkiympäristönä vastaaville organisaatioille. Projektissa toteutettu työ syvensi kaikkien projektiin osallistuneiden henkilöiden tietämystä ja osaamista tietoturvaratkaisujen toteuttamisesta verkkoympäristöissä, joissa on toteutettuna useamman eri kategorian verkkopalveluita ja -rakenteita.

Lähteet

1 Security threat report 2012. 2012. Verkkodokumentti. Sophos Ltd. [http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf]. Luettu 10.2.2012.

2 A look back at 2011 information is currency. 2012. Verkkodokumentti. Trend micro Inc. [http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_a-look-back-at-2011_information-is-currency.pdf]. Luettu 2.3.2012.

3 Tietoturva nyt! 11/2011. 5.11.2011. Verkkodokumentti. CERT.FI. [http://www.cert.fi/tietoturvanyt/2011/11/ttn201111051616.html]. Luettu 19.1.2012.

4 Mustonen, Erkki. 2012. Tietokone 02/2012, s. 15.

5 Kotilainen, Samuli. Helenius, Timo. 2011. Yhden laitteen turvaa. Tietokone 07/2011, s. 48-54.

6 Facebook: Measuring the cost to business of social notworking. 2009. Verkkodokumentti. Nucleusresearch Inc. [http://nucleusresearch.com/research/notes-and-reports/facebook-measuring-the-cost-to-business-of-social-notworking]. Luettu 7.3.2012.

7 Accelerating UTM with specialized hardware. 2011. Verkkodokumentti. Fortinet Inc. [http://www.fortinet.com/sites/default/files/whitepapers/Accelerating_UTM_Specialized_Hardware.pdf]. Luettu 27.8.2011.

8 FortiOS Handbook v3. 2011. Verkkodokumentti. Fortinet Inc. [http://docs.fortinet.com/fgt/handbook/40mr3/fortios-handbook-40-mr3.pdf]. Luettu 20.3.2012.

9 Fortiguard intrusion prevention system. 2012. Verkkodokumentti. Fortinet Inc. [http://www.fortinet.com/support/fortiguard_services/ips.html]. Luettu 16.2.2012.

10 Password recovery speeds. 2009. Verkkodokumentti. Lockdown. [http://www.lockdown.co.uk/?pg=combi] Luettu 29.1.2012.

11 Requirements for Internet hosts – communication layers. 1989. Verkkodokumentti. IETF. [http://tools.ietf.org/pdf/rfc1122.pdf]. Luettu 7.1.2012.

12 FortiGate-310/311B. 2012. Verkkodokumentti. Fortinet Inc. [http://www.fortinet.com/products/fortigate/310B.html]. Luettu 13.1.2011.

13 Securelist local infections. 2012. Verkkodokumentti. Kaspersky Lab ZEO. [http://www.securelist.com/en/statistics#/en/top20/oas/month]. Luettu 3.3.2012.

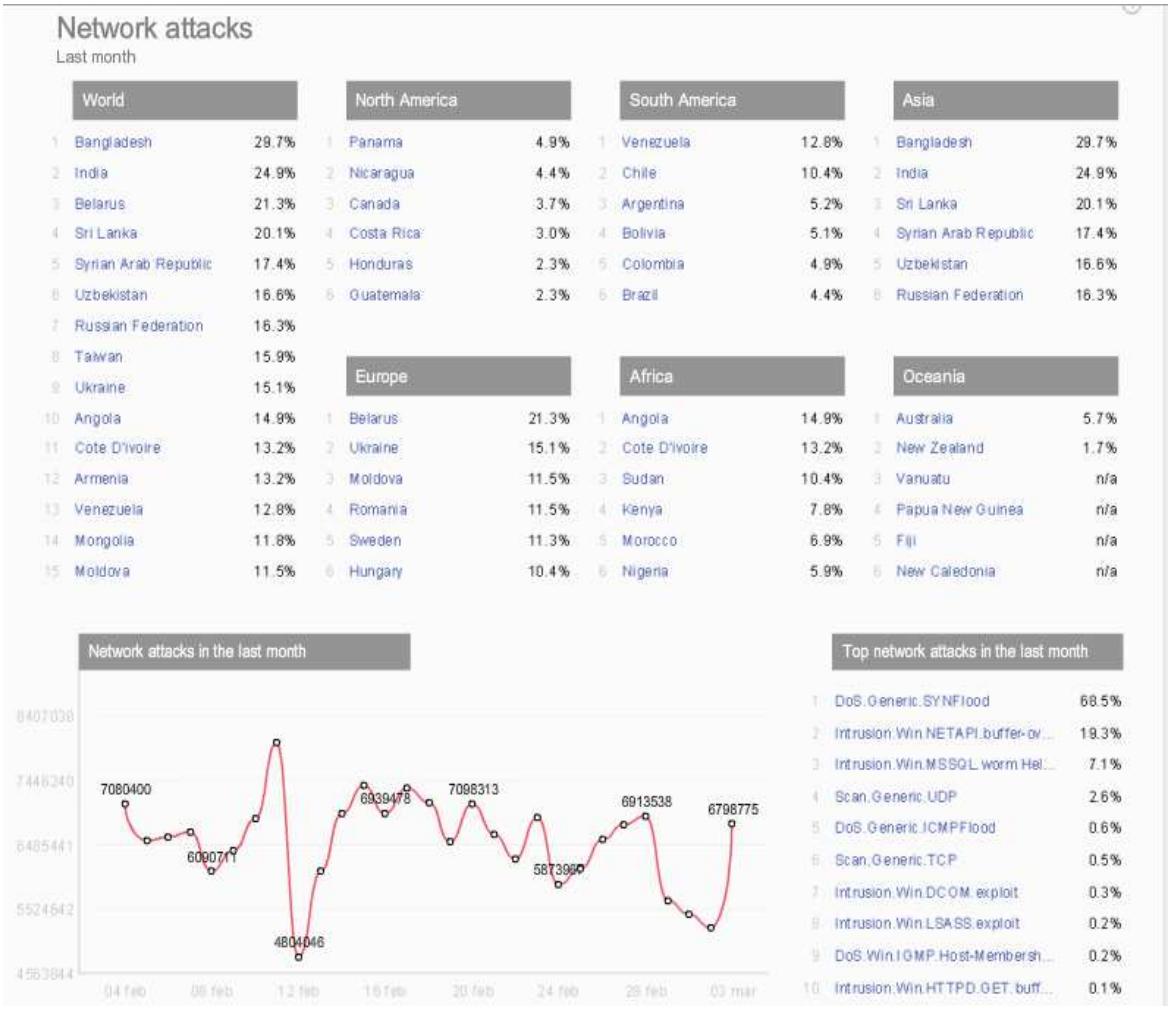
14 Securelist network attacks. 2012. Verkkodokumentti. Kaspersky Lab ZEO. [http://www.securelist.com/en/statistics#/en/top20/ids/month]. Luettu 3.3.2012.

15 Securelist vulnerabilities. 2012. Verkkodokumentti. Kaspersky Lab ZEO. [http://www.securelist.com/en/statistics#/en/top20/vul/month]. Luettu 3.3.2012.

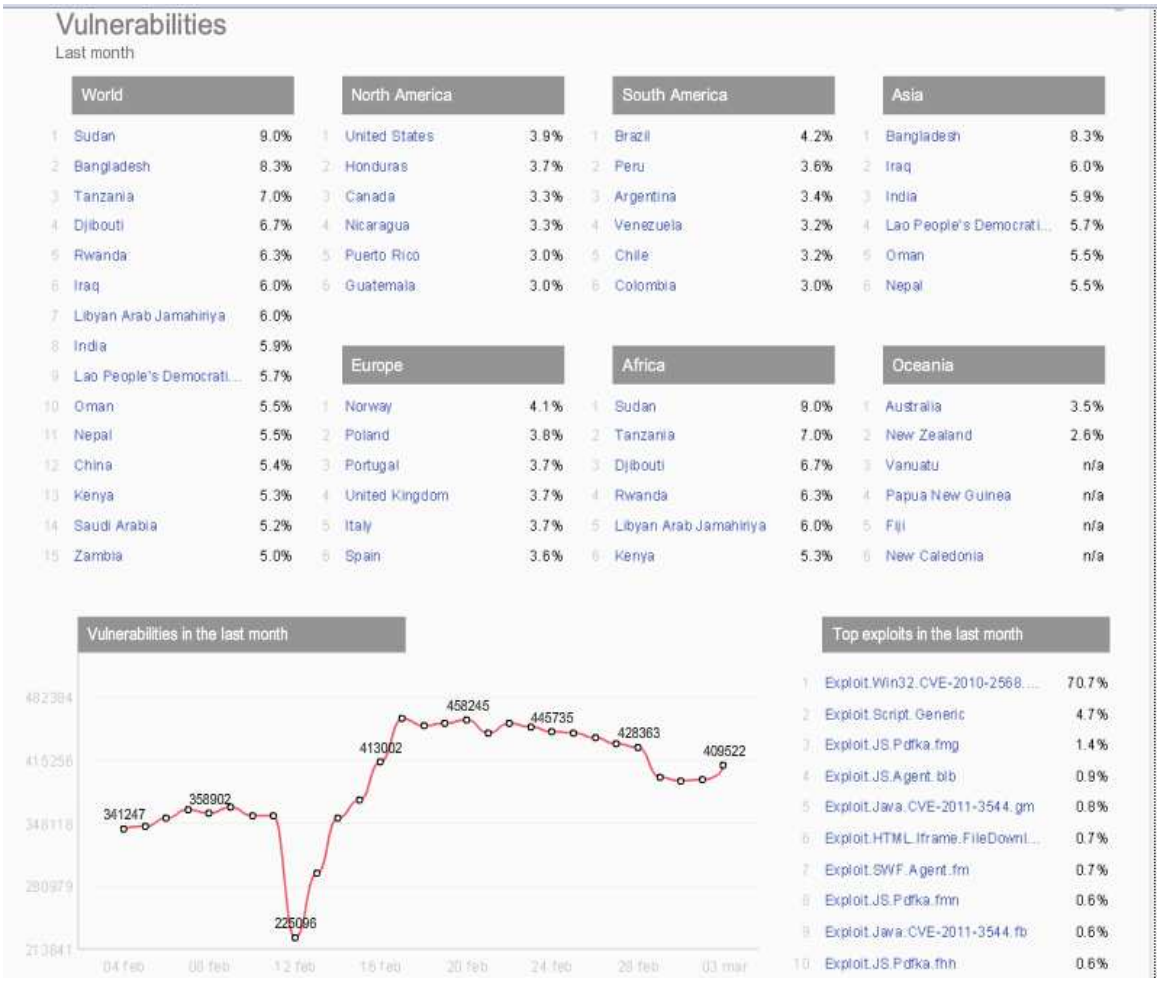
16 Life of a packet. 2008. Verkkodokumentti. Fortinet Inc. [http://docs.fortinet.com/fgt/archives/3.0/techdocs/Life_of_a_Packet_01-30006-0146-20080111.pdf]. Luettu 5.12.2012.

Kaspersky-tietoturvalaboratorion statistiikka

Kuvio 21. Saastuneiden laitteiden määrä 02/2012 [13].

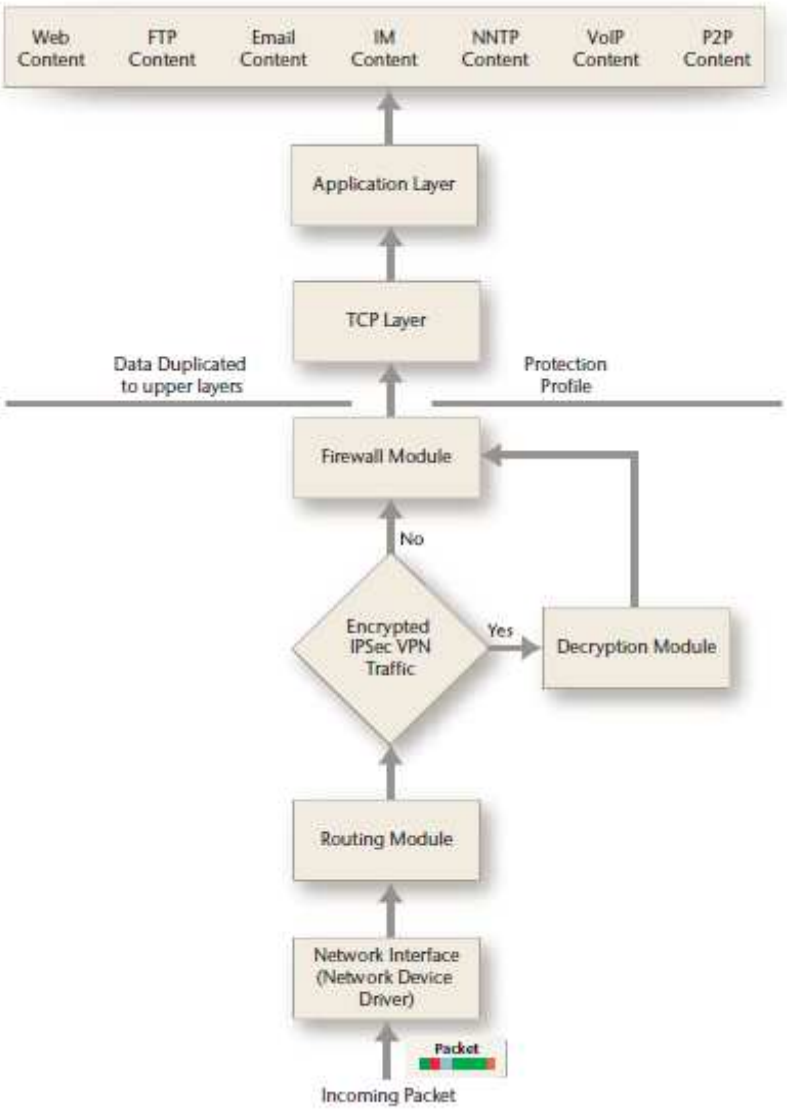


Kuvio 22. Verkkohyökkäykset 02/2012 [14].

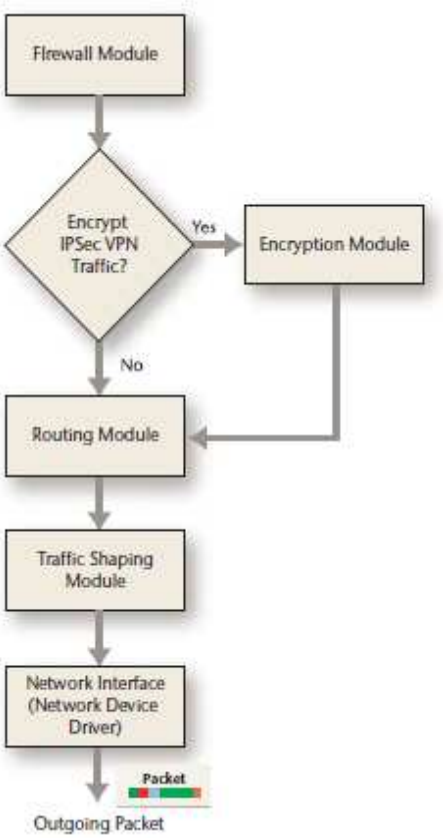


Kuvio 23. Haavoittuvuudet 02/2012 [15].

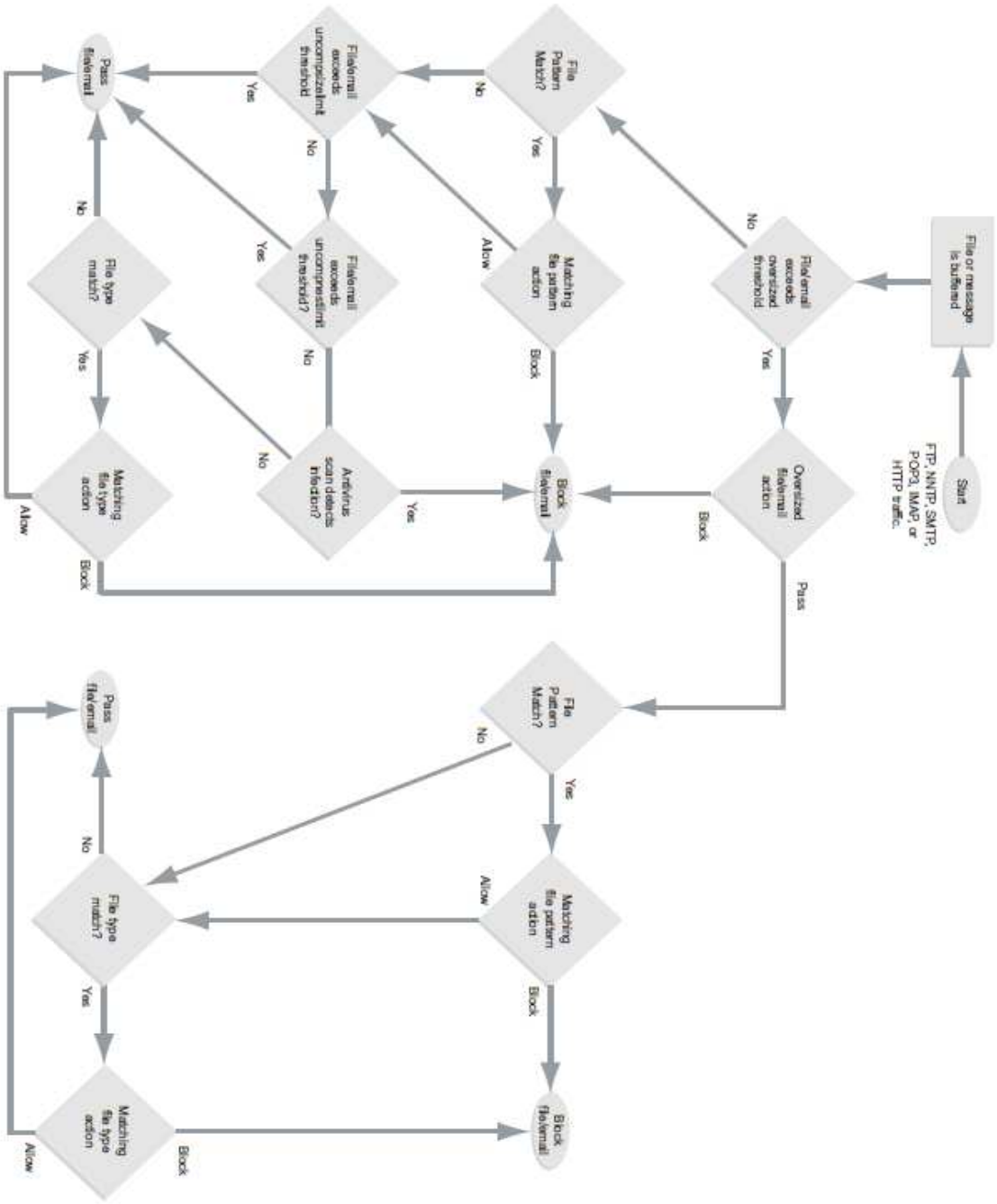
FortiGate-prosessikaaviot



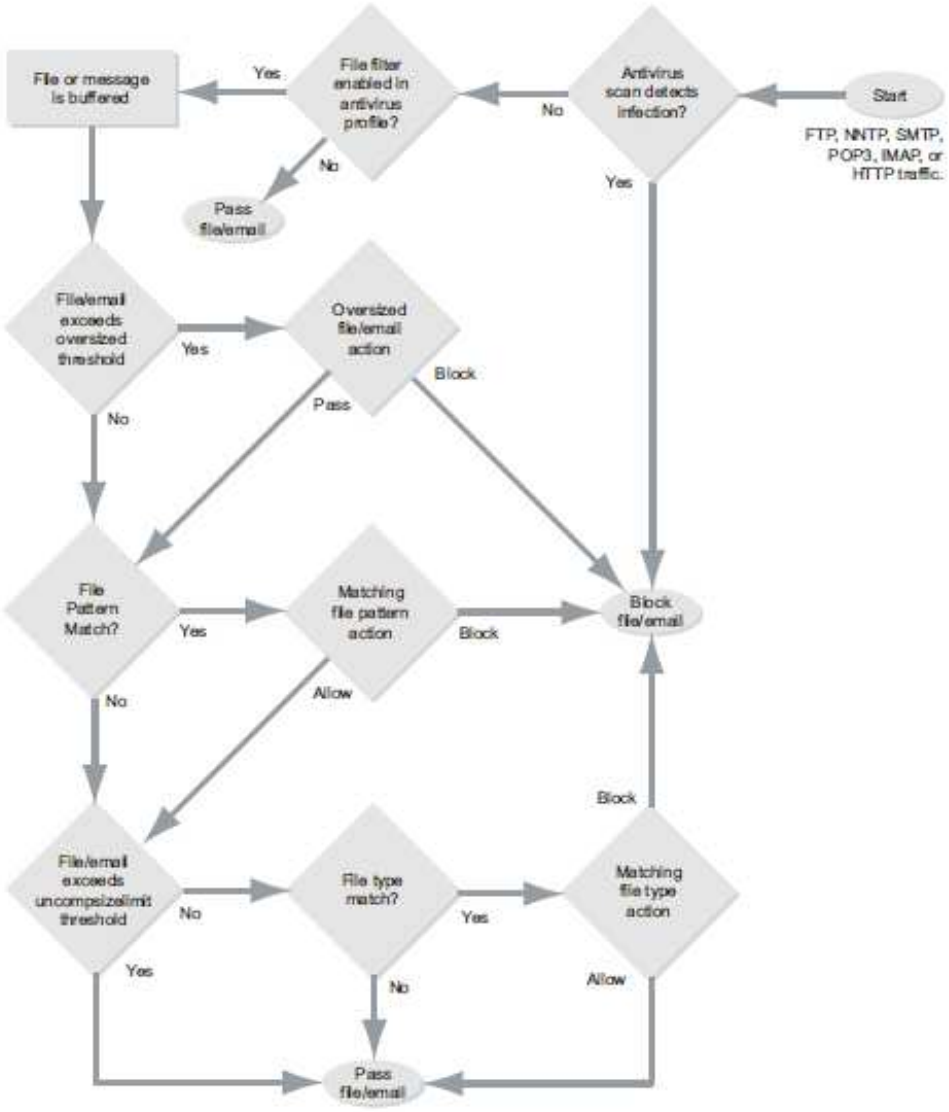
Kuvio 24. FortiGate-palomuurin reititysprosessi saapuvalle liikenteelle [16, s. 6].



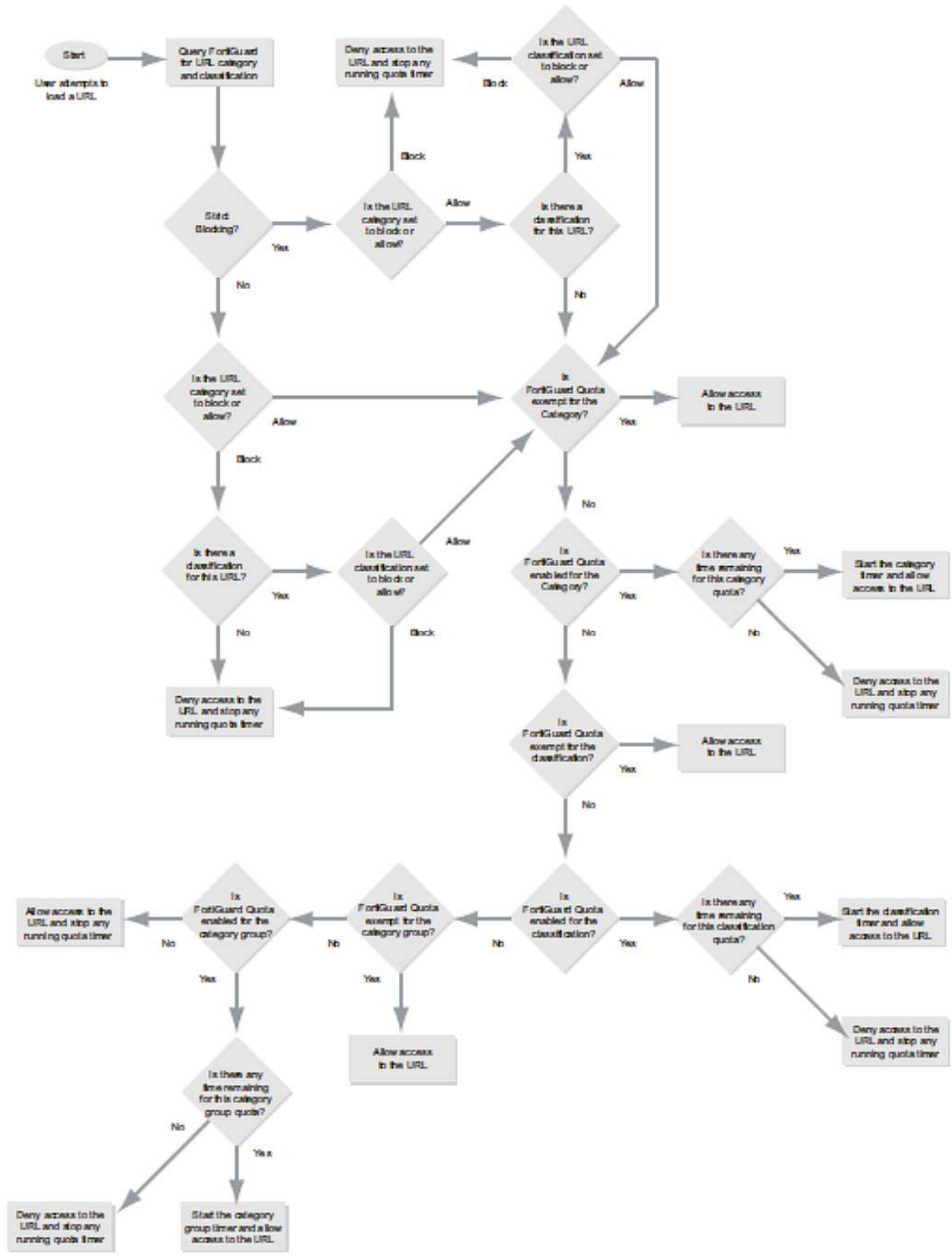
Kuvio 25. FortiGate-palomuurin reitityksprosessi lähtevälle liikenteelle [16, s. 14].



Kuvio 26. FortiGate antiviruksen puskuroidun skannauksen prosessikaavio [8, s. 785].



Kuvio 27. FortiGate antiviruksen lennosta suoritettavan skannauksen prosessikaavio [8, s. 786].



Kuvio 28. FortiGate web-suodattimen prosessikaavio [8, s. 863].